目　　錄

第一章　整數之分解 …… 1

§1　整除性 …… 1
§2　素數及複合數 …… 2
§3　素數 …… 3
§4　整數之模 …… 4
§5　唯一分解定理 …… 6
§6　最大公因數及最小公倍數 …… 7
§7　逐步淘汰原則 …… 9
§8　一次不定方程之解 …… 11
§9　完全數 …… 13
§10　Mersenne 數及 Fermat 數 …… 14
§11　連乘積中素因數之方次數 …… 15
§12　整値多項式 …… 17
§13　多項式之分解 …… 19

第二章　同餘式 …… 22

§1　定義 …… 22
§2　同餘式之基本性質 …… 22
§3　縮剩餘系 …… 24
§4　p^2 可整除 $2^{p-1}-1$ 否? …… 25
§5　$\varphi(m)$ 之討論 …… 28
§6　同餘方程 …… 30
§7　孫子定理 …… 32
§8　高次同餘式 …… 34
§9　素數乘方爲模之高次同餘方程 …… 35
§10　Wolstenholme 定理 …… 37

第三章　二次剩餘 …… 38

§1　定義及 Euler 判別條件 …… 38
§2　計算法則 …… 40
§3　互逆定律 …… 42
§4　實際算法 …… 46

§ 5　二次同餘式之根數 …… 48
§ 6　Jacobi 符號 …… 49
§ 7　二項同餘式 …… 52
§ 8　原根及指數 …… 54
§ 9　縮系之構造 …… 56

第四章　多項式之性質 …… 66

§ 1　多項式之整除性 …… 66
§ 2　唯一分解定理 …… 68
§ 3　同餘式 …… 70
§ 4　整係數多項式 …… 72
§ 5　以素數爲模之多項式 …… 73
§ 6　若干關於分解之定理 …… 75
§ 7　重模同餘式 …… 78
§ 8　Fermat 定理之推廣 …… 79
§ 9　對模 p 之不可化多項式 …… 81
§ 10　原根 …… 82
§ 11　總結 …… 83

第五章　素數分佈之概況 …… 85

§ 1　無窮大之階 …… 85
§ 2　對數函數 …… 86
§ 3　引言 …… 87
§ 4　素數之個數無限 …… 90
§ 5　幾乎全部整數皆非素數 …… 93
§ 6　Чебышев 定理 …… 94
§ 7　Bertrand 假設 …… 97
§ 8　以積分來估計和之數值 …… 100
§ 9　Чебышев 定理之推論 …… 103
§ 10　n 之素因子的個數 …… 108
§ 11　表素數之函數 …… 111
§ 12　等差級數中之素數問題 …… 112

第六章　數論函數 …… 115

§ 1　數論函數舉例 …… 115
§ 2　積性函數之性質 …… 117
§ 3　Möbius 反轉公式 …… 118
§ 4　Möbius 變換 …… 121

§ 5　除數函數 …… 124
§ 6　關於概率之二定理 …… 127
§ 7　表整數爲二平方之和 …… 129
§ 8　分部求和法及分部積分法 …… 135
§ 9　圓內整點問題 …… 137
§ 10　Farey 貫及其應用 …… 140
§ 11　**Виноградов** 關於函數的分數部分和的估值定理 …… 145
§ 12　**Виноградов** 定理對整點問題之應用 …… 149
§ 13　Ω-結果 …… 153
§ 14　Dirichlet 級數 …… 159
§ 15　Lambert 級數 …… 162

第 七 章　三角和及特徵 …… 164

§ 1　剩餘系之表示法 …… 164
§ 2　特徵函數 …… 166
§ 3　特徵之分類 …… 172
§ 4　特徵和 …… 175
§ 5　Gauss 和 …… 178
§ 6　特徵和與三角和 …… 185
§ 7　由完整和到不完整和 …… 186
§ 8　特徵和 $\sum_{x=1}^{p}\left(\frac{x^2+ax+b}{p}\right)$ 之應用舉例 …… 190
§ 9　原根之分佈問題 …… 193
§ 10　含多項式之三角和 …… 196

第 八 章　與橢圓模函數有關的幾個數論問題 …… 202

§ 1　引言 …… 202
§ 2　整數分拆 …… 203
§ 3　Jacobi 等式 …… 204
§ 4　分式表示法 …… 209
§ 5　分拆之圖解法 …… 211
§ 6　$p(n)$ 之估值 …… 214
§ 7　平方和問題 …… 220
§ 8　密率 …… 226
§ 9　關於平方和問題之總結 …… 232

第 九 章　素數定理 …… 234

§ 1　引言 …… 234

§ 2 Riemann ζ 函數 …… 236
§ 3 若干引理 …… 239
§ 4 Tauber 型定理 …… 242
§ 5 素數定理 …… 246
§ 6 Selberg 漸近公式 …… 248
§ 7 素數定理的初等證明 …… 250
§ 8 Dirichlet 定理 …… 258

第十章 漸近法與連分數 …… 264

§ 1 簡單連分數 …… 264
§ 2 連分數展開之唯一性 …… 268
§ 3 最佳漸近分數 …… 271
§ 4 Hurwitz 定理 …… 272
§ 5 實數之相似 …… 275
§ 6 循環連分數 …… 280
§ 7 Legendre 之判斷條件 …… 282
§ 8 二次不定方程 …… 284
§ 9 Pell 氏方程 …… 286
§ 10 Чебышев 定理及 Хинчин 定理 …… 289
§ 11 一致分佈及 $n\vartheta \pmod 1$ 之一致分佈性 …… 293
§ 12 一致分佈之判斷條件 …… 295

第十一章 不定方程 …… 301

§ 1 引言 …… 301
§ 2 一次不定方程 …… 301
§ 3 二次不定方程 …… 303
§ 4 解 $ax^2+bxy+cy^2=k$ …… 304
§ 5 求解方法 …… 309
§ 6 商高 定理之推廣 …… 313
§ 7 Fermat 猜測 …… 318
§ 8 Марков 方程 …… 320
§ 9 解方程 $x^3+y^3+z^3+w^3=0$ …… 322
§ 10 三次曲面之有理點 …… 326

第十二章 二元二次型 …… 334

§ 1 二元二次型之分類 …… 334
§ 2 類數有限 …… 336
§ 3 Kronecker 符號 …… 339

§ 4 二次型表整數之表法數 …… 341
§ 5 二次型的 mod q 相似 …… 343
§ 6 二次型的特徵系．族 …… 348
§ 7 級數 $K(d)$ 之收斂性 …… 350
§ 8 雙曲扇形及橢圓內的整點數 …… 352
§ 9 平均極限 …… 353
§ 10 類數的解析表示法 …… 356
§ 11 基本判別式 …… 356
§ 12 類數公式 …… 357
§ 13 Pell 氏方程的最小解 …… 361
§ 14 若干引理 …… 364
§ 15 Siegel 定理 …… 366

第十三章 模變換 …… 372

§ 1 複虛數平面 …… 372
§ 2 線性變換之性質 …… 373
§ 3 線性變換下之幾何性質 …… 376
§ 4 實變換 …… 377
§ 5 模變換 …… 382
§ 6 基域 …… 383
§ 7 基域網 …… 387
§ 8 模羣之構造 …… 388
§ 9 二次定正型 …… 389
§ 10 二次不定型 …… 390
§ 11 二次不定型的極小值 …… 393

第十四章 整數矩陣及其應用 …… 398

§ 1 引言 …… 398
§ 2 矩陣之積 …… 404
§ 3 模方陣之演出元素 …… 410
§ 4 左結合 …… 414
§ 5 不變因子．初等因子 …… 416
§ 6 應用 …… 419
§ 7 因子分解．標準素方陣 …… 420
§ 8 最大公約．最小公倍 …… 425
§ 9 線性模 …… 429

第十五章　p-adic 數 …… 435
§ 1　引言 …… 435
§ 2　賦值之定義 …… 438
§ 3　賦值之分類 …… 440
§ 4　亞幾米得賦值 …… 442
§ 5　非亞幾米得賦值 …… 443
§ 6　有理數之 ϕ-擴張 …… 446
§ 7　擴張之完整性 …… 450
§ 8　p-adic 數之表示法 …… 452
§ 9　應用 …… 456
第十六章　代數數論介紹 …… 458
§ 1　代數數 …… 458
§ 2　代數數域 …… 460
§ 3　基底 …… 462
§ 4　整底 …… 466
§ 5　整除性 …… 470
§ 6　理想數 …… 474
§ 7　理想數的唯一分解定理 …… 476
§ 8　理想數的基底 …… 481
§ 9　同餘關係 …… 483
§ 10　素理想數 …… 484
§ 11　單位數 …… 489
§ 12　理想數類 …… 490
§ 13　二次域與二次型 …… 492
§ 14　族 …… 497
§ 15　歐幾里得域與單域 …… 499
§ 16　判斷 Mersenne 數是否素數之 Lucas 條件 …… 501
§ 17　不定方程 …… 503
§ 18　表 …… 509
第十七章　代數數與超越數 …… 529
§ 1　超越數之存在定理 …… 529
§ 2　Liouville 定理及超越數例子 …… 531
§ 3　代數數的有理逼近定理 …… 533
§ 4　Roth 定理之應用 …… 553
§ 5　Thue 定理之應用 …… 555
§ 6　e 之超越性 …… 558

§ 7　π 之超越性 ······ 561
§ 8　Hilbert 第七問題 ······ 563
§ 9　Гельфонд 之證明 ······ 566

第十八章　Waring 問題及 Prouhet-Tarry 問題 ······ 569

§ 1　引言 ······ 569
§ 2　$g(k)$ 及 $G(k)$ 之下限 ······ 569
§ 3　Cauchy 定理 ······ 571
§ 4　初等方法示例 ······ 574
§ 5　有正負號之較易問題 ······ 578
§ 6　等冪和問題 ······ 580
§ 7　Prouhet-Tarry 問題 ······ 582
§ 8　續 ······ 586

第十九章　Шнирельман 密率 ······ 588

§ 1　密率之定義及其歷史 ······ 588
§ 2　和集及其密率 ······ 589
§ 3　Гольдбах-Шнирельман 定理 ······ 592
§ 4　Selberg 不等式 ······ 593
§ 5　Гольдбах-Шнирельман 定理之證明 ······ 599
§ 6　Waring-Hilbert 定理 ······ 603
§ 7　Waring-Hilbert 定理的證明 ······ 605

第二十章　數的幾何 ······ 609

§ 1　二維空間之情况 ······ 609
§ 2　Minkowski 之基本定理 ······ 612
§ 3　一次線性式 ······ 613
§ 4　二次定正型 ······ 615
§ 5　線性型之乘積 ······ 617
§ 6　聯立漸近法 ······ 619
§ 7　Minkowski 不等式 ······ 620
§ 8　線性型之乘方平均值 ······ 627
§ 9　Чеботарев 定理 ······ 629
§ 10　在代數數論上的應用 ······ 631
§ 11　$|\Delta|$ 的極小值 ······ 634

參考書目 ······ 639
名詞索引 ······ 641

第 一 章

整 數 之 分 解

在本章中，如無特別聲明，常以小寫拉丁字母

$$a, b, \cdots, n, \cdots, p, \cdots, x, y, z$$

代表整數. 本章之目的在證明唯一分解定理 (定理 5.3), 並旁及其應用.

§1. 整除性. 自然數是指 1, 2, 3, … 之一而言；整數乃指

$$\cdots, -2, -1, 0, 1, 2, \cdots$$

之一而言. 故自然數卽正整數. 顯然二整數之和、差、積仍爲整數. 此項性質可述爲："諸整數所成之集，對加、減、乘三種運算自封".

命 α 爲一實數. 今後常以 $[\alpha]$ 表最大之整數不超過 α 者. 例如

$$[3]=3, \quad [\sqrt{2}]=1, \quad [\pi]=3, \quad [-\pi]=-4.$$

若 α 爲正，易見 $[\alpha]$ 卽爲 α 之整數部分；顯然有下之不等式:

$$[\alpha] \leqslant \alpha < [\alpha]+1.$$

今取 α 爲有理數 $\frac{a}{b}$, $b>0$, 則有

$$0 \leqslant \frac{a}{b}-\left[\frac{a}{b}\right]<1,$$

卽

$$0 \leqslant a-b\left[\frac{a}{b}\right]<b.$$

立得

$$a=\left[\frac{a}{b}\right] b+r, \quad 0 \leqslant r<b.$$

由此可得:

定理 1. 任與二整數 a 及 b $(b>0)$, 必有二整數 q 及 r 使

$$a=qb+r, \quad 0 \leqslant r<b.$$

r 名爲以 b 除 a 所得之最小剩餘.

定義. 若最小剩餘爲 0, 則 a 名爲 b 之倍數. 換言之,若有一整數 c, 使得

$$a = bc,$$

則謂 b 可整除 a; a 稱爲 b 之倍數, b 稱爲 a 之因數,以

$$b \mid a$$

表之. 故顯然有

$$1 \mid a, \quad b \mid 0.$$

對任一 $a \neq 0$ 有

$$a \mid a.$$

又以

$$b \nmid a$$

表示 b 不能整除 a.

若 $a = bc$, 而 b 既非 a 又非 1, 則 b 稱爲 a 之眞因數.

關於整除性,顯然有下列定理:

定理 2. 若 $b \neq 0$, $c \neq 0$, 則

1) 若 $b \mid a$, $c \mid b$, 則 $c \mid a$;

2) 若 $b \mid a$, 則 $bc \mid ac$;

3) 若 $c \mid d$, $c \mid e$, 則對任意的 m. n, 有

$$c \mid dm + en.$$

定理 3. 若 b 是 a 的眞因數,則

$$1 < |b| < |a|.$$

習題 1. 若 n 爲正整數,則 $\left[\frac{[n\alpha]}{n} \right] = [\alpha]$.

習題 2. 若 n 爲正整數,則

$$[\alpha] + \left[\alpha + \frac{1}{n}\right] + \cdots + \left[\alpha + \frac{n-1}{n}\right] = [n\alpha].$$

習題 3. 證明不等式

$$[2\alpha] + [2\beta] \geqslant [\alpha] + [\alpha + \beta] + [\beta].$$

§2. 素數及複合數. 今將自然數分爲三類:

(i) 1, 只有自然數 1 爲其因數;

(ii) p, 恰有二自然數 1 及 p 爲其因數. 換言之, p 乃大於 1 且無眞因數之自然數;

(iii) n, 有眞因數之自然數. (此類之數,有兩個以上的因數.)

第二類數名爲素數 (prime), 第三類數名爲複合數 (composite number). 吾人常以 p 表素數.

2 所能整除之數謂之偶數; 非偶數之整數名爲奇數. 顯然大於 2 之偶數皆非素數.

定理 1. 非 1 之自然數皆可分解爲素數之積.

證: 若 n 爲素數,自毋待言. 今設 n 非素數,而 q_1 爲其最小眞因數. 由定理 1.3, 可知 q_1 爲素數. 命

$$n = q_1 n_1, \quad 1 < n_1 < n.$$

若 n_1 已爲素數,自毋待言;不然,則命 q_2 爲 n_1 之最小素因數,而得

$$n = q_1 q_2 n_2, \quad 1 < n_2 < n_1 < n.$$

續行此法,得 $n > n_1 > n_2 > \cdots > 1$. 此項手續,不能超過 n 次,故最後必得

$$n = q_1 q_2 \cdots q_s,$$

其中 $q_1, \cdots, q_s$ 皆爲素數. 定理已明.

例如: $10725 = 3^1 \cdot 5^2 \cdot 11^1 \cdot 13^1$.

將定理 1 中所得之素因數排成

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \quad a_1 > 0, a_2 > 0, \cdots, a_k > 0,$$

$$p_1 < p_2 < \cdots < p_k.$$

此式名爲 n 之標準分解式,或標準表示法.

標準分解式之唯一性,卽所謂"算術基本定理",將在 §5 中論證之.

§3. 素數. 最初之若干素數爲

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, …

若 N 並不太大,求小於 N 之諸素數,並非難事. 有所謂 Eratosthenes 氏篩法者. 若 $n \leqslant N$, 而 n 非素數,則 n 必爲一不大於 $\sqrt{N}$ 之素數所整除. 先列下所有不超過 N 之整數:

$$2,3,4,5,6,\cdots,N.$$

陸續除去:

(i) 4, 6, 8, 10, ⋯ 即由 2^2 起之一切偶數;

(ii) 9, 15, 21, 27, ⋯ 即由 3^2 起之一切 3 的倍數;

(iii) 25, 35, 55, 65, ⋯ 即由 5^2 起之一切 5 的倍數;⋯

繼續行之,待不大於 $\sqrt{N}$ 之素數之倍數,概行除去以後,所餘者即爲不大於 N 之素數. 現在所做出之素數表,無一不由此法略加變化而得者.

素數表之最準確者爲 Lehmer 氏表: List of prime numbers from 1 to 10,006,721, Carnegie Institution, Washington 165 (1914).

Lehmer 還著有因數分解表: Factor table for the first ten millions, Carnegie Institution, Washington 105 (1909).

我們已知一個 39 位的素數

$$2^{127}-1=1701,41183,46046,92317,31687,30371,58841,05727.$$

而

$$180\,(2^{127}-1)^2+1$$

則是一個 79 位的素數.

至目前爲止,所知道的最大的素數爲 $2^{2281}-1$, 共 687 位.

$$2^{257}-1=231,58417,84746,32390,84714,19700,17375,81570,$$
$$65399,69331,28112,80789,15168,01582,62592,79871.$$

此乃最大之複合數,而未能覓出其分解式者. 證明時皆需機械幫助並用特殊方法. 本書中將敍述證明此諸事實之方法,但不涉及其冗長計算 (見 §3.9 及 §16.15). 玆將 5,000 以內之素數表附在第三章之末.

§4. 整數之模. 模 (modulus) 者乃對加減自封之一數集. 換言之,若 m 及 n 皆在一模中,則 $m\pm n$ 亦屬此模. 只有 0 之模謂之零模. 又如全體整數成一模. 凡 k 之倍數也成一模.

今所討論者乃僅有整數之模. 由定義易知:

定理 1.

1) 任何模中必含有 0;

2) 若 a, b 在模中,則 $am+bn$ 亦然, m, n 爲任何整數.

證: 1) 模中任取一數 a, 則 $0=a-a$ 在模中.

2) 若 a 在模中, 則 $2a=a+a$, $3a=2a+a$, $\cdots$, ma 皆在模中. 同樣 nb 亦在模中. 故得定理.

定理 2. 任與二整數 a 及 b, 則所有形如 $am+bn$ 之整數成一模.

此定理至爲明顯,毋須證明.

定理 3. 任一非零之模,必爲一正整數之諸倍數所成之集合.

證: 命 d 爲此模中之最小正整數, 則其他之數必爲此 d 之倍數. 因若不然,設 n 在模中而非 d 之倍數,則由定理 1.1, 有二整數 q 及 r 使

$$n=dq+r,\qquad 1\leqslant r<d.$$

由模之定義,可知 $r=n-dq$ 在此模中; 此與 d 之原假定之性質相違背. 故模內其他各數必爲 d 之倍數. 又若 d 在模中,則 d 之倍數亦在模中. 定理已明.

定義. 命 a, b 爲二整數. 於定理 3 中取形如 $am+bn$ 所成之模, 則此定理證明中所得之 d 名爲 a, b 之最大公因數, 以 (a,b) 表之.

定理 4. (a,b) 有如下性質:

(i) 有整數 x, y, 使 $(a,b)=ax+by$;

(ii) 對任二整數 x, y, 必有 $(a,b)|ax+by$;

(iii) 若 $e|a$, $e|b$, 則 $e|(a,b)$.

(由 (iii) 可知,最大公因數卽最大的公共因數.)

證: (i) 及 (ii) 可由定理 4.3 立刻推得, (iii) 可由 (i) 直接推得.

定義. 若 $(a,b)=1$, 則 a, b 謂之互素.

附言: 在定理 3 之證明中, 實已提示一通常所熟知之求最大公因數法, 卽輾轉相除法. 此亦名爲 Euclid 計算法. 我國秦九韶於數學九章 (1247 年) 中亦論及之.

例. 取 $a=323$, $b=221$. 由 Euclid 算法可得

$$323=221\cdot 1+102.$$

故 102 在形如 $ax+by$ 之整數模中. 又

$$221=102\cdot 2+17,$$

故 17 亦在模中. 因

$$102 = 17 \cdot 6,$$

故 17 爲該模之最小正整數,卽 $17 = (323, 221)$. 用此法可求出定理 4 (i) 中之 x 及 y. 因

$$\begin{aligned} 17 &= 221 - 2 \cdot 102 \\ &= 221 - 2(323 - 221) \\ &= 3 \cdot 221 - 2 \cdot 323, \end{aligned}$$

故 $x = -2$, $y = 3$.

此法肇源極古,乃初等數論之主要支柱之一.

§5. 唯一分解定理.

定理 1. 若 p 爲素數且 $p|ab$, 則 $p|a$, 或 $p|b$.

證: 若 $p \nmid a$, 則 $(a, p) = 1$. 由定理 4.4, 知有二整數 x, y, 使

$$xa + yp = 1.$$

故

$$x \cdot ab + yb \cdot p = b.$$

但 $p \mid ab$, 故 $p \mid b$.

定理 2. 若 $c > 0$, 及 $(a, b) = d$, 則 $(ac, bc) = dc$.

證: 有 x 及 y 使

$$xa + yb = d,$$

或

$$xac + ybc = dc,$$

故 $(ac, bc)|dc$. 另一方面, 由 $d|a$,可得 $cd|ca$; 同樣, $cd|cb$. 故 $dc|(ac,bc)$. 合此二結論立得定理.

定理 3. n 之標準分解式是唯一的. 換言之,若不計次序,則 n 僅能由唯一之方法表爲素數之積.

證: 由定理 1 顯然可知,若

$$p|abc\cdots l,$$

則 p 必整除 $a, b, c, \cdots, l$ 中之一. 特如 $a, b, c, \cdots, l$ 皆爲素數,則 p 必爲 $a, b, c, \cdots, l$ 中之一.

假定

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \cdots q_j^{b_j}$$

為 n 之二種標準分解式，則由上述原則，任一 p 必為 q 中之一，而任一 q 亦必為 p 中之一． 故 $k = j$． 且由

$$p_1 < p_2 < \cdots < p_k, \quad q_1 < q_2 < \cdots < q_k,$$

可知

$$p_i = q_i, \qquad 1 \leqslant i \leqslant k.$$

若 $a_i > b_i$，則以 $p_i^{b_i}$ 除之，可得

$$p_1^{a_1} \cdots p_i^{a_i - b_i} \cdots p_k^{a_k} = p_1^{b_1} \cdots p_{i-1}^{b_{i-1}} p_{i+1}^{b_{i+1}} \cdots p_k^{b_k}$$

左邊為 p_i 之倍數，而右邊則否，此不可能．同樣 $a_i < b_i$ 也不可能．故 $a_i = b_i$，而得定理．

此處順帶說明不視 1 為素數之道理． 因為如把 1 視為素數，則在 n 之標準分解式前，可乘以 1 之任何次冪，而唯一性被破壞矣．

習題 1. 證明以下各數非有理數(有理數者乃形如 $\frac{a}{b}$ 之數)．

$$\log_{10} 2, \qquad \sqrt{2}.$$

習題 2. 若已知

$$\log_{10} \frac{1025}{1024} = a, \quad \log_{10} \frac{1024^2}{1023 \cdot 1025} = b, \quad \log_{10} \frac{81^2}{80 \cdot 82} = c,$$

$$\log_{10} \frac{125^2}{124 \cdot 126} = d, \qquad \log_{10} \frac{99^2}{98 \cdot 100} = e,$$

則

$$196 \log_{10} 2 = 59 + 5a + 8b - 3c - 8d + 4e.$$

並試用 a, b, c, d, e 表出 $\log_{10} 3$ 及 $\log_{10} 41$；再用此法以求 $\log_{10} 2$ 至小數第十位，以說明此法在實際計算上有用處． (已知 $\log_e 10 = 2.3025850930$.)

§6. 最大公因數及最小公倍數．

定理 1. 命 a, b 為二正整數，$p_1, \cdots, p_s$ 為其素因數，書

$$a = p_1^{a_1} \cdots p_s^{a_s}, \qquad a_\nu \geqslant 0,$$
$$b = p_1^{b_1} \cdots p_s^{b_s}, \qquad b_\nu \geqslant 0, \qquad p_1 < p_2 < \cdots < p_s,$$

則

$$(a, b) = p_1^{c_1} \cdots p_s^{c_s},$$

其中 $c_\nu=\min(a_\nu, b_\nu)$. 此處及今後將以 $\min(x_1, \cdots, x_n)$ 表 n 個數 $x_1, \cdots, x_n$ 中之最小者.

此定理乃屬顯然.

定義. 命 a, b 為二正整數, a, b 皆能整除之數,謂之 a, b 之公倍數;其中之最小正數名為最小公倍數. 公倍數之存在,並無問題,因 ab 即為其一; 故最小公倍數之存在,亦無問題.

定理 2. 如定理 1 之假定, a, b 之最小公倍數為

$$e=p_1^{e_1}\cdots p_s^{e_s},$$

其中 $e_\nu=\max(a_\nu, b_\nu)$. 此處及今後將以 $\max(x_1, \cdots, x_n)$ 表 n 個數 $x_1, \cdots, x_n$ 中之最大者.

證: 顯然 e 可為 a 及 b 所整除. 反之,若

$$e'=p_1^{m_1}\cdots p_s^{m_s}$$

可為 a 所整除,則 $a_\nu \leqslant m_\nu$. 故若 e' 可為 a 及 b 所整除,則 $a_\nu \leqslant m_\nu$, $b_\nu \leqslant m_\nu$, 即 $\max(a_\nu, b_\nu) \leqslant m_\nu$. 故 $e \mid e'$. 即得定理.

顯然可得:

定理 3. a, b 之任一公倍數必為其最小公倍數之倍數.

定理 4. 以 $[a, b]$ 表 a, b 之最小公倍數,則

$$[a, b](a, b)=ab.$$

證: 命

$$a=p_1^{a_1}\cdots p_s^{a_s}, \quad b=p_1^{b_1}\cdots p_s^{b_s}, \qquad p_1<p_2<\cdots<p_s.$$

則

$$ab=p_1^{a_1+b_1}\cdots p_s^{a_s+b_s}.$$

又

$$[a, b](a, b)=p_1^{\max(a_1, b_1)+\min(a_1, b_1)}\cdots p_s^{\max(a_s, b_s)+\min(a_s, b_s)}.$$

故只須證明

$$x+y=\max(x, y)+\min(x, y)$$

即是. 但此乃顯然,故得定理.

今用歸納法定義多個數之最大公因數及最小公倍數. $a_1, \cdots, a_n$ 之最大公因數為

$$(a_1, \cdots, a_n) = ((a_1, \cdots, a_{n-1}), a_n);$$

其最小公倍數爲

$$[a_1, \cdots, a_n] = [[a_1, \cdots, a_{n-1}], a_n].$$

定理 5. 命

$$a_1 = p_1^{e_{11}} \cdots p_s^{e_{1s}}, \cdots, a_n = p_1^{e_{n1}} \cdots p_s^{e_{ns}},$$

$$p_1 < p_2 < \cdots < p_s, \quad e_{\mu\nu} \geqslant 0,$$

則

$$(a_1, \cdots, a_n) = p_1^{e_1} \cdots p_s^{e_s}, \qquad e_\nu = \min(e_{1\nu}, \cdots, e_{n\nu}),$$

$$[a_1, \cdots, a_n] = p_1^{d_1} \cdots p_s^{d_s}, \qquad d_\nu = \max(e_{1\nu}, \cdots, e_{n\nu}).$$

讀者自證.

習題 1. 證明下列二等式:

$$(a_1, \cdots, a_n) = ((a_1, \cdots, a_s), (a_{s+1}, \cdots, a_n)),$$

$$[b_1, \cdots, b_n] = [[b_1, \cdots, b_s], [b_{s+1}, \cdots, b_n]].$$

習題 2. 證明下列二式:

$$(a_1, \cdots, a_n) = \frac{a_1 a_2 \cdots a_n}{[a_2 \cdots a_n, a_1 a_3 \cdots a_n, \cdots, a_1 \cdots a_{n-1}]},$$

$$[a_1, \cdots, a_n] = \frac{a_1 a_2 \cdots a_n}{(a_2 \cdots a_n, a_1 a_3 \cdots a_n, \cdots, a_1 \cdots a_{n-1})}.$$

習題 3. 命 $a_1, \cdots, a_n$ 爲 n 個整數,則 $(a_1, \cdots, a_n)$ 爲形如 $a_1x_1 + \cdots + a_nx_n$ 諸整數所成之模中之最小正整數.

習題 4. 求出一組 x, y, z 使

$$6x + 15y + 20z = 17.$$

習題 5. 今有散錢不知其數,作七十七陌穿之,欠五十湊穿,若作七十八陌穿之,不多不少. 問錢數若干. (答: 2106) 嚴恭,通原算法 (1372).

§7. 逐步淘汰原則.

定理 1. 設有 N 件事物,其中 N_α 件有性質 α, N_β 件有性質 $\beta, \cdots$, $N_{\alpha\beta}$ 件兼有性質 α 及 $\beta, \cdots$, $N_{\alpha\beta\gamma}$ 件兼有性質 α, β 及 $\gamma, \cdots$. 則此事物中之既無性質 α, 又無性質 β, 又無性質 $\gamma, \cdots$ 者之件數爲

(A)
$$N - N_\alpha - N_\beta - \cdots$$
$$+ N_{\alpha\beta} + \cdots$$

$$- N_{\alpha\beta\gamma} - \cdots$$
$$+ \cdots - \cdots.$$

證: 命 P 爲一事物之兼有 k 種性質 $\alpha, \beta, \cdots$ 者. 則 P 於 N 中出現一次; 於 $N_\alpha, N_\beta, \cdots$ 中出現 k 次;於 $N_{\alpha\beta}, \cdots$ 中出現 $\binom{k}{2} = \frac{1}{2}k(k-1)$ 次;於 $N_{\alpha\beta\gamma}, \cdots$ 中出現 $\binom{k}{3} = \frac{1}{6}k(k-1)(k-2)$ 次; $\cdots$. 若 $k \geqslant 1$, 則於 (A) 中共出現

$$1 - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} \cdots = (1-1)^k = 0$$

次. 但若 $k = 0$, 則無 $\alpha, \beta, \gamma, \cdots$ 諸性質之 P 於 (A) 中出現之次數爲 1. 故得所云.

今應用此原則: "性質 α" 視爲 "不大於 a", $\cdots$, 可得:

定理 2. 若 $a, b, \cdots, k, l$ 爲任意非負之數,則

$$\begin{aligned}\max(a, b, \cdots, k, l) = {} & a + b + \cdots + k + l \\ & - \min(a, b) \cdots - \min(k, l) \\ & + \min(a, b, c) + \cdots \\ & - \cdots + \cdots \\ & \pm \min(a, b, \cdots, k, l).\end{aligned}$$

證: 取最初 $N(> \max(a, b, \cdots, k, l))$ 個正整數. 無性質 $\alpha, \beta, \cdots$ 之數之個數爲 $N - \max(a, b, \cdots, k, l)$. 此後應用定理 1 卽得.

由此可推得:

定理 3.

$$[a_1, \cdots, a_n] = a_1 \cdots a_n (a_1, a_2)^{-1} \cdots (a_{n-1}, a_n)^{-1} (a_1, a_2, a_3) \cdots (a_1, \cdots, a_n)^{(-1)^{n+1}}.$$

讀者可自證之. 同様可得:

定理 4.

$$(a_1, \cdots, a_n) = a_1 \cdots a_n [a_1, a_2]^{-1} \cdots [a_{n-1}, a_n]^{-1} [a_1, a_2, a_3] \cdots [a_1, \cdots a_n]^{(-1)^{n+1}}.$$

附言: §6 之習題 1, 2 及定理 7.3 及 7.4 建立一 "對偶原則" (principle of duality) 卽 ( ) 與 [ ] 可以互換.

習題. 命 $a, b, \cdots, k, l$ 爲正整數,求 $1, 2, \cdots, n$ 中與 $a, b, \cdots, l$ 皆互素之整數之個數.

§8. **一次不定方程之解.** 由定理 4.4 可知:

定理 1. 方程

$$ax + by = n$$

有整數解 x, y 的必要且充分之條件爲 $(a, b) \mid n$.

定理 2. 若 $(a, b) = 1$, 且 x_0, y_0 爲

$$ax + by = n \tag{1}$$

之一解(此解之存在無問題),則 (1) 式之解皆可表爲

$$x = x_0 + bt, \quad y = y_0 - at.$$

且對任何整數 t, 此皆 (1) 式之解.

證: 由

$$ax + by = n$$

及

$$ax_0 + by_0 = n$$

可得

$$a(x - x_0) + b(y - y_0) = 0.$$

因 $(a, b) = 1$, 故 $a \mid y - y_0$. 命

$$y = y_0 - at,$$

則

$$x = x_0 + bt;$$

以此代入 (1) 式,顯然適合.

定理 3. 設 $(a, b) = 1$, $a > 0$, $b > 0$. 凡大於 $ab - a - b$ 之數必可表爲 $ax + by (x \geqslant 0, y \geqslant 0)$ 之形. 但 $ab - a - b$ 不能表成此形.

證: 由定理 2 可知

$$n = ax + by$$

之解必爲

$$x = x_0 + bt, \quad y = y_0 - at$$

之形. 今求 t 使 x 及 y 都非負數. 可取 t 之值使

$$0 \leqslant y_0 - at < a,$$

即

$$0 \leqslant y_0 - at \leqslant a - 1.$$

由假定可知

$$(x_0+bt)a=n-(y_0-at)b>ab-a-b-(a-1)b=-a,$$

即

$$x_0+bt>-1,$$

故

$$x_0+bt\geqslant 0.$$

又若

$$ab-a-b=ax+by,\quad x\geqslant 0,\quad y\geqslant 0,$$

則

$$ab=(x+1)a+(y+1)b.$$

因 $(a,b)=1$，故

$$a\mid(y+1),\quad b\mid(x+1),$$

即

$$y+1\geqslant a,\quad x+1\geqslant b.$$

立得

$$ab=(x+1)a+(y+1)b\geqslant 2ab.$$

此不可能.

以上定理亦可述爲：若 $a>0$, $b>0$, $(a,b)=1$, 則 $ab-a-b$ 爲最大之整數不能由 $ax+by$ ($x\geqslant 0, y\geqslant 0$) 表出者. 推廣此問題至三個變數：命 a,b,c 爲三正整數, 且 $(a,b,c)=1$, 求最大之整數不可由 $ax+by+cz$ ($x\geqslant 0$, $y\geqslant 0$, $z\geqslant 0$) 表出者. 此乃一未經解決之問題.

習題 1. 若 $a>0$, $b>0$, 且 $(a,b)=1$, 則方程

$$ax+by=n$$

之非負數解答之個數爲 $\left[\frac{n}{ab}\right]$ 或 $\left[\frac{n}{ab}\right]+1$.

[提示：應用 $[\alpha]-[\beta]=[\alpha-\beta]$ 或 $[\alpha-\beta]+1$.]

習題 2. 設 a,b,c 爲三正整數, 且

$$(a,b)=(b,c)=(c,a)=1.$$

求最大之整數之不可由

$$bcx+cay+abz,\quad x\geqslant 0,\quad y\geqslant 0,\quad z\geqslant 0$$

表出者. (答：$2abc-ab-bc-ca$).

習題 3. 求出 $x+2y+3z=n$, $x\geqslant 0$, $y\geqslant 0$, $z\geqslant 0$ 之解數.

[提示: 此式之解答數爲

$$\frac{1}{(1-x)(1-x^2)(1-x^3)}$$

之展開式中 x^n 之係數. 用部分分式法可得所需.]

$$\left(答: \frac{(n+3)^2}{12}-\frac{7}{72}+\frac{(-1)^n}{8}+\frac{2}{9}\cos\frac{2n\pi}{3}.\right)$$

習題 4. 鷄翁一,值錢五; 鷄母一,值錢三; 鷄雛三,值錢一. 百錢買鷄百隻,問鷄翁、母、雛各幾何? (張丘建).

§ 9. 完全數 (perfect number).

定理 1. 命 $\sigma(n)$ 爲 n 之諸因數之和. 若 $n=p_1^{a_1}\cdots p_s^{a_s}$, 則

$$\sigma(n)=\frac{p_1^{a_1+1}-1}{p_1-1}\cdots\frac{p_s^{a_s+1}-1}{p_s-1}.$$

證: 顯然

$$p_1^{x_1}\cdots p_s^{x_s}, \qquad 0\leqslant x_1\leqslant a_1, \cdots, \quad 0\leqslant x_s\leqslant a_s$$

爲 n 之所有的因數,而無其他. 故

$$\sigma(n)=\sum_{x_1=0}^{a_1}\cdots\sum_{x_s=0}^{a_s}p_1^{x_1}\cdots p_s^{x_s}=$$

$$=\sum_{x_1=0}^{a_1}p_1^{x_1}\cdot\sum_{x_2=0}^{a_2}p_2^{x_2}\cdots\sum_{x_s=0}^{a_s}p_s^{x_s}=$$

$$=\frac{p_1^{a_1+1}-1}{p_1-1}\cdots\frac{p_s^{a_s+1}-1}{p_s-1}.$$

顯然立刻可得

定理 2. 若 $(n, m)=1$, 則

$$\sigma(m\,n)=\sigma(m)\,\sigma(n).$$

附言: 此種 $\sigma(n)$ 乃所謂數論函數之一種. 數論函數之有定理 2 之性質者, 謂之積性函數 (multiplicative function).

定義. 若 $\sigma(n)=2n$, 則 n 謂之完全數. 例如:

$$6=1+2+3, \quad 28=1+2+4+7+14.$$

定理 3. 若 $p=2^n-1$ 爲素數,則

$$\frac{1}{2}p(p+1)=2^{n-1}(2^n-1)$$

乃一完全數,且無其他偶完全數存在.

證: 1) 由定理 1 知

$$\sigma\left(\frac{1}{2}p(p+1)\right)=\frac{2^n-1}{2-1}\frac{p^2-1}{p-1}=(2^n-1)(p+1)=p(p+1).$$

2) 若 a 爲一偶完全數. 命

$$a=2^{n-1}u,\quad u>1,\ 2\nmid u,$$

則由定理 2,

$$2^n u=2a=\sigma(a)=\frac{2^n-1}{2-1}\sigma(u),$$

故

$$\sigma(u)=\frac{2^n u}{2^n-1}=u+\frac{u}{2^n-1}.$$

但 u 及 $\frac{u}{2^n-1}$ 皆爲 u 之因數. 而 $\sigma(u)$ 爲 u 的所有因數之和. 故 u 祇有兩個因數,卽 u 爲素數,且

$$\frac{u}{2^n-1}=1.$$

定理於是證明.

習題 1. 闡明 $\sigma(m)=\sigma(n)=m+n$ 有次之三解答:

m	284	17296	9363584
n	220	18416	9437056

習題 2. 求證: 若一正整數爲其諸因數(除其本身之外)之積,則此數爲一素數之立方,或爲二不同素數之積,且無其他正整數具此性質.

§10. Mersenne 數及 Fermat 數. 是否有奇完全數存在,乃數論中之著名難題. 由上節之結果可知,偶完全數之問題一變而爲求形如 2^n-1 之素數之問題. 此種素數乃所謂 Mersenne 數. 有一 Mersenne 數卽有一偶完全數. 是否有無窮個 Mersenne 數存在,亦爲數論上之難題.

定理 1. 若 $n>1$, 且 a^n-1 爲素數,則 $a=2$, 及 n 爲素數.

證: 若 $a>2$, 則 $(a-1)\mid(a^n-1)$. 故 a^n-1 非素數.

若 $a=2$ 而 $n=kl$, 則 $(2^k-1)\mid(2^n-1)$.

故 2^n-1 爲素數之問題,今已化爲 2^p-1 爲素數之問題. 命

$$M_p = 2^p - 1$$

表示 Mersenne 數. 迄今所已證明之結果爲: 當

$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281$

時 M_p 爲素數. 卽迄今所知者,僅十七個偶完全數而已.

與 Mersenne 數有相似形式者,有所謂 Fermat 數,此對分圓問題,甚有用處.

定理 2. 若 $2^m + 1$ 爲素數,則 $m = 2^n$.

證: 若 m 有一奇因子 q, 命 $m = qr$, 則

$$2^{qr} + 1 = (2^r)^q + 1 = (2^r + 1)(2^{r(q-1)} - \cdots + 1),$$

而 $1 < 2^r + 1 < 2^{qr} + 1$. 故 $2^m + 1$ 非素數.

命 $F_n = 2^{2^n} + 1$. 此名爲 Fermat 數. 最前五個 Fermat 數是

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537;$$

都是素數. 根據此種事實, Fermat 猜測凡 F_n 皆爲素數. 但 Euler 於 1732 年舉出

$$F_5 = 2^{2^5} + 1 = 641 \times 6700417.$$

故 Fermat 之猜測並不眞確.

附註: "$641 \mid F_5$" 可簡證如次: 命 $a = 2^7$, $b = 5$, 則 $a - b^3 = 3$, $1 + ab - b^4 = 1 + 3b = 2^4$. 故

$$2^{2^5} + 1 = (2a)^4 + 1 = (1 + ab - b^4)a^4 + 1 = (1 + ab)a^4 + 1 - a^4 b^4.$$

此必爲 $1 + ab$ 所整除. 而 $1 + ab = 2^4 + 5^4 = 641$.

近若干年來關於 Fermat 數之結果,總結如次: 當

$$n = 6, 7, 8, 9, 11, 12, 18, 23, 36, 38, 73,$$

F_n 皆非素數. 故除了開始之五素數外, 是否尙有 F_n 爲素數之情形存在, 實可懷疑. 故 Fermat 此一推測實屬不幸之至. 今已有反推測 "Fermat 數僅有有限個素數存在" 者矣.

Gauss 曾證明: 若 F_n 爲素數,則正 F_n 角形可用圓規及直尺作出. 故 Fermat 數之爲素數之問題,在幾何學上有其特殊的應用.

§11. 連乘積中素因數之方次數.

定理 1. 命 p 爲一素數. 於 $n!$ 中 p 之方次數等於

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\cdots.$$

此級數中僅有有限項不等於零.

證: 於

$$n!=1\cdot 2\cdots(p-1)\cdot$$
$$\cdot p\cdot(p+1)\cdots 2p\cdots(p-1)p\cdots\cdot$$
$$\cdot p^2\cdots\cdot$$
$$\cdots\cdots\cdots$$

中有 $\left[\frac{n}{p}\right]$ 個 p 之倍數,有 $\left[\frac{n}{p^2}\right]$ 個 p^2 之倍數,等等. 故得定理.

定理 2. 命

$$\binom{n}{r}=\frac{n!}{r!(n-r)!}.$$

此爲一整數.

證: 今將利用下之公式

$$[\alpha]-[\beta]=[\alpha-\beta] \text{ 或 } [\alpha-\beta]+1. \tag{1}$$

其證明極易(且已於習題 8.1 中用及之). 由定理 1, 於 $\binom{n}{r}$ 中 p 之方次數爲

$$\sum\left(\left[\frac{n}{p^m}\right]-\left[\frac{r}{p^m}\right]-\left[\frac{n-r}{p^m}\right]\right).$$

由 (1) 可知此式 $\geqslant 0$.

例. 若 $n=1000$, $p=3$, 則

$$\left[\frac{1000}{3}\right]=333,\left[\frac{1000}{3^2}\right]=\left[\frac{333}{3}\right]=111,\left[\frac{1000}{3^3}\right]=37,$$
$$\left[\frac{1000}{3^4}\right]=12,\left[\frac{1000}{3^5}\right]=4,\left[\frac{1000}{3^6}\right]=1.$$

故 1000! 中 3 之方次數爲

$$333+111+37+12+4+1=498.$$

習題 1. 求 10000! 中 7 之方次數.

習題 2. 求 $\binom{1000}{500}$ 中 5 之方次數.

習題 3. 若 $r+s+\cdots+t=n$, 則

$$\frac{n!}{r!\,s!\cdots t!}$$

爲整數. 更證明若 n 爲素數,而 $\max(r, s, \cdots, t) < n$, 則此數爲 n 之倍數.

§ 12. **整值多項式.**

定義. 當變數 x 爲整數時,若一多項式 $f(x)$ 之值常爲整數,則此種多項式謂之整值多項式.

例如: 整係數之多項式爲整值多項式. 又如

$$\binom{x}{r} = \frac{x(x-1)\cdots(x-r+1)}{r!}$$

亦爲整值多項式.

以 $\Delta f(x)$ 表 $f(x+1) - f(x)$, 則有

定理 1. $\Delta\binom{x}{r} = \binom{x}{r-1}$.

證: $$\Delta\binom{x}{r} = \frac{(x+1)\,x\cdots(x-r+2)}{r!} - \frac{x(x-1)\cdots(x-r+1)}{r!} =$$
$$= \frac{x\cdots(x-r+2)}{r!}\Big((x+1)-(x-r+1)\Big) = \binom{x}{r-1}.$$

定理 2. 凡 k 次之整值多項式必可表成

$$a_k\binom{x}{k} + a_{k-1}\binom{x}{k-1} + \cdots + a_1\binom{x}{1} + a_0;$$

式中 $a_k, \cdots, a_0$ 皆爲整數. 且對任何整數 $a_k, \cdots, a_0$, 此皆整值多項式.

證: 1) 如此之多項式顯然是整值多項式.

2) 任一 k 次多項式 $f(x)$ 必可寫成

$$f(x) = \alpha_k\binom{x}{k} + \alpha_{k-1}\binom{x}{k-1} + \cdots + \alpha_1\binom{x}{1} + \alpha_0.$$

顯然

$$\Delta f(x) = \alpha_k\binom{x}{k-1} + \alpha_{k-1}\binom{x}{k-2} + \cdots + \alpha_1.$$

進而以 $\Delta^2 f(x)$ 表 $\Delta(\Delta f(x))$, 及 $\Delta^r f(x) = \Delta(\Delta^{r-1} f(x))$, 可立得

$$f(0) = \alpha_0, \quad (\Delta f(x))_{x=0} = \alpha_1, \cdots, \quad (\Delta^r f(x))_{x=0} = \alpha_r, \cdots.$$

若 $f(x)$ 爲整值多項式, 則 $\Delta f(x)$, $\Delta^2 f(x)$, $\cdots$ 亦然. 故 $f(0)$, $(\Delta f(x))_{x=0}$, $\cdots$, $(\Delta^r f(x))_{x=0}$, $\cdots$ 皆爲整數,即 $\alpha_k, \cdots, \alpha_0$ 皆爲整數.

定理 3. 對任意整數 x，一整值多項式 $f(x)$ 之值皆爲 m 之倍數之必要且充分條件爲

$$m \mid (a_k, \cdots, a_0);$$

此處 $a_k, \cdots, a_0$ 之意義如定理 2.

證法與定理 2 同.

定理 4 (Fermat). 命 p 爲一素數，對任一整數 x，$x^p - x$ 必爲 p 之倍數.

證：若 $p=2$，則由 $x^2 - x = x(x-1)$，定理顯然. 故可設 $p>2$.

命 $f(x) = x^p - x$. 顯然 $f(0) = 0$ 及

$$\triangle f(x) = (x+1)^p - x^p - (x+1) + x =$$
$$= \binom{p}{1} x^{p-1} + \binom{p}{2} x^{p-2} + \cdots + \binom{p}{p-1} x,$$

此式中之係數皆爲 p 之倍數（習題 11.3）. 以 0 代入，$f(1)$ 爲 p 之倍數；以 1 代入，$f(2)$ 爲 p 之倍數；等等. 故 $f(x)$ 之值常爲 p 之倍數. 若 x 爲負整數，則由 $x^p - x = -[(-x)^p - (-x)]$，定理顯然成立.

習題 1. 推廣定理 2 及 3 至多變數之情形.

習題 2. 證明 $n(n+1)(2n+1)$ 是 6 之倍數.

習題 3. 當 m 及 n 過諸正整數時，

$$m + \frac{1}{2}(m+n-1)(m+n-2)$$

亦過諸正整數，既無遺漏，也無重複.

習題 4. 若一 k 次多項式，對於連續 $k+1$ 個整數皆取整數值，則此多項式必爲整值多項式.

習題 5. 若 $f(-x) = -f(x)$，則 $f(x)$ 名爲奇多項式. 整值奇多項式之形式爲

$$a_1\binom{x}{1} + a_2\binom{x+1}{3} + \cdots + a_m\binom{x+m-1}{2m-1}.$$

此處 $a_1, \cdots, a_m$ 爲整數.

習題 6. 若 $f(-x) = f(x)$，則 $f(x)$ 名爲偶多項式. 整值偶多項式之形式爲

$$a_0 + a_1 \frac{x}{1}\binom{x}{1} + a_2 \frac{x}{2}\binom{x+1}{3} + \cdots + a_m \frac{x}{m}\binom{x+m-1}{2m-1}.$$

此處 $a_1, \cdots, a_m$ 爲整數.

§ 13. **多項式之分解.**

定理 1. 命 $g(x)$ 及 $h(x)$ 爲二整係數多項式:

$$g(x) = a_l x^l + \cdots + a_0, \qquad a_l \neq 0,$$
$$h(x) = b_m x^m + \cdots + b_0, \qquad b_m \neq 0,$$

及

$$g(x)\, h(x) = c_{l+m} x^{l+m} + \cdots + c_0.$$

則

$$(a_l, \cdots, a_0)(b_m, \cdots, b_0) = (c_{l+m}, \cdots, c_0).$$

證: 可假定 $(a_l, \cdots, a_0) = 1$, $(b_m, \cdots, b_0) = 1$ 而不失其普遍性.

設 $p \mid (c_{l+m}, \cdots, c_0)$ 及

$$p \mid (a_l, \cdots, a_{u+1}), \qquad p \nmid a_u,$$
$$p \mid (b_m, \cdots, b_{v+1}), \qquad p \nmid b_v.$$

由定義可得

$$c_{u+v} = \sum_{s+t=u+v} a_s b_t.$$

其中除 $a_u b_v$ 一項之外,皆爲 p 之倍數. 因 $p \nmid a_u b_v$, 故 $p \nmid c_{u+v}$, 故 $p \nmid (c_{l+m}, \cdots, c_0)$. 此與假定相違背. 故任何素數皆不能整除 $(c_{l+m}, \cdots, c_0)$.

定義. 命 $f(x)$ 爲一有理係數多項式, 若有二非常數之有理係數多項式 $g(x)$ 及 $h(x)$ 使

$$f(x) = g(x)\, h(x).$$

則 $f(x)$ 謂之可分解或可化 (reducible). 不然, 則謂之不可分解或不可化 (irreducible).

例. $x^2 - 2$ 及 $x^2 + 1$ 皆爲不可化; 而 $3x^2 + 8x + 4$ 爲可化,因其可分解爲 $(3x+2)(x+2)$.

定理 2 (Gauss). 命 $f(x)$ 爲一整係數多項式. 若

$$f(x) = g(x)\, h(x),$$

此處 $g(x)$, $h(x)$ 爲二有理係數多項式. 則有一有理數 γ 使

$$\gamma g(x),\ \frac{1}{\gamma}h(x)$$

皆有整係數.

證: 可假定 $f(x)$ 之係數之最大公因數是 1. 有二整數 M 及 N 使

$$M g(x) = a_l x^l + \cdots + a_0, \qquad \text{諸 } a \text{ 爲整數};$$
$$N h(x) = b_m x^m + \cdots + b_0, \qquad \text{諸 } b \text{ 爲整數};$$
$$M N f(x) = c_{l+m} x^{l+m} + \cdots + c_0.$$

由假定及定理 1 可知

$$M N = (c_{l+m}, \cdots, c_0) = (a_l, \cdots, a_0)(b_m, \cdots, b_0).$$

命

$$\gamma = \frac{M}{(a_l, \cdots, a_0)} = \frac{(b_m, \cdots, b_0)}{N},$$

則 $\gamma g(x)$ 及 $\frac{1}{\gamma}h(x)$ 皆有整係數.

定 理 3 (Eisenstein). 命

$$f(x) = c_n x^n + \cdots + c_0$$

爲一整係數多項式. 若 $p \nmid c_n$, $p \mid c_i$ $(0 \leqslant i < n)$, 且 $p^2 \nmid c_0$, 則 $f(x)$ 爲不可化.

證: 假定 $f(x)$ 爲可化. 由定理 2 可知

$$f(x) = g(x)\,h(x),$$
$$g(x) = a_l x^l + \cdots + a_0, \qquad h(x) = b_m x^m + \cdots + b_0,$$
$$l + m = n, \qquad l > 0, \qquad m > 0,$$

式中 a_i 及 b_k 皆爲整數. 由 $c_0 = a_0 b_0$ 及 $p \mid c_0$, 可知 $p \mid a_0$ 或 $p \mid b_0$. 設 $p \mid a_0$, 則由 $p^2 \nmid a_0 b_0 = c_0$ 可得 $p \nmid b_0$.

又 $g(x)$ 之係數不能皆爲 p 之倍數,因若不然,則 $p \mid c_n$. 故可假定

$$p \mid (a_0, \cdots, a_{r-1}), \qquad p \nmid a_r, \qquad 1 \leqslant r \leqslant l.$$

由

$$c_r = a_r b_0 + \cdots + a_0 b_r.$$

可知 $p \nmid c_r$. 因 $r \leqslant l < n$, 此與假定相違背.

由此定理,立得以下諸結果:

定理 4. $x^m - p$ 爲不可化. 故 $\sqrt[m]{p}$ 爲無理數.

定理 5. $\frac{x^p-1}{x-1} = x^{p-1} + \cdots + x + 1$ 爲不可化.

證: 命 $x = y + 1$, 則上式變爲

$$\frac{1}{y}((y+1)^p - 1) = y^{p-1} + p\,y^{p-2} + \binom{p}{2} y^{p-3} + \cdots + p.$$

易見除第一係數外,皆爲 p 之倍數,而常數項非 p^2 之倍數.

習題. 證明次之諸式皆不可化:

$$x^2 + 1, \quad x^4 + 1, \quad x^6 + x^3 + 1.$$

第　二　章

同　餘　式

§1. 定義. 命 m 爲一自然數,若 $a-b$ 爲 m 之倍數,則謂之"a, b 對模 m 同餘 (congruent)". 以

$$a \equiv b \pmod m$$

表示之. 反之,以

$$a \not\equiv b \pmod m$$

表示 a 與 b 對模 m 不同餘.

例如: $31 \equiv -9 \pmod{10}$.

對任二整數 a 及 b, 常有

$$a \equiv b \pmod 1.$$

同餘之觀念,在日常生活中,時常用及. 例如:"星期三上課一次", 卽有此觀念, 其所用之模爲七. 又我國古時所創之干支紀年也屬此類, 卽以 60 爲模之紀年法也. 我國對此問題有極光榮之歷史,如孫子算經有"物不知其數"一問, 卽爲同餘式研究之濫觴. 此問題之原文如次:

今有物不知其數,三三數之賸二,五五數之賸三,七七數之賸二,問物幾何?

用以上所述之符號表之,卽爲求正整數 x 使

$$x \equiv 2 \pmod 3,$$

$$x \equiv 3 \pmod 5,$$

$$x \equiv 2 \pmod 7.$$

故"物不知其數"問題,卽爲求若干個同餘式之公解也.

§2. 同餘式之基本性質.

定理 1.

(i) $a \equiv a \pmod m$ (反身性);

(ii) 若 $a \equiv b \pmod m$, 則

$b \equiv a \pmod{m}$（對稱性）;

(iii) 若 $a \equiv b,\ b \equiv c \pmod{m}$，則

$a \equiv c \pmod{m}$（傳遞性）.

此三性質之證明極易，不再贅述. 由此三項性質可以分整數爲若干類，同類之數皆同餘，異類者皆不同餘，此項之類，名爲同餘類（residue class）. 顯然，如以 m 爲模，吾人有 m 個同餘類：爲 m 所整除之諸數成一類，以 m 除餘 1 之數成一類，餘 2 之數成一類，等等.

每類中各取一數爲代表，此代表組名爲一完全剩餘系(complete residue system).

定理 2. 若

$$a \equiv b, \quad a_1 \equiv b_1 \pmod{m},$$

則

$$a + a_1 \equiv b + b_1, \quad a - a_1 \equiv b - b_1 \pmod{m},$$

及

$$a\,a_1 \equiv b\,b_1 \pmod{m}.$$

此定理之證明，亦不困難，今僅舉最後一式之證明：

$$m \mid a_1(a-b) + b(a_1 - b_1) = aa_1 - bb_1.$$

定理 2 也可改述如次：任與二類 A, B，其中各取一代表 a 及 b，命 $a+b$（或 $a-b$，或 ab）所代表之類爲 C. 則 C 僅與 A, B 有關，而與其所取之代表無關. 亦卽 A, B 中各取一數，其和必在 C 中. 故可定義類 C 爲類 A 類 B 之和. 以 $C = A + B$ 表之. 同樣，可以定義 $A - B$ 及 $A \cdot B$. 由定理 2 也可推得"對模 m 之諸類，對加減乘自封". 但對除法不一定可能，例如 $3 \cdot 2 \equiv$ $\equiv 1 \cdot 2,\ 2 \equiv 2 \pmod{4}$，但 $3 \not\equiv 1 \pmod{4}$. 惟吾人有次之定理：

定理 3. 若

$$ac \equiv bd \pmod{m}$$

$$c \equiv d \pmod{m}$$

及 $(c, m) = 1$，則

$$a \equiv b \pmod{m}.$$

證： 由

$$(a-b)\,c + b\,(c-d) = ac - bd \equiv 0 \pmod{m}$$

可得

$$m \mid (a-b)\,c.$$

但 $(c, m) = 1$, 故得

$$m \mid a - b.$$

以 0 表諸 m 之倍數所成之類. 易知

$$A + 0 = A, \quad A \cdot 0 = 0.$$

又以 I 表以 m 除餘 1 諸數所成之類,易見

$$A \cdot I = A.$$

前例及定理 3 說明: 由

$$A \cdot B = A \cdot C$$

不一定可得 $B = C$. 但 A 中之數與 m 爲互素(注意:如 A 中有一數與 m 互素,則其他諸數也與 m 互素),則可得 $B = C$.

如取 m 爲素數 p, 則除 0 之外, 其他之類皆與 m 互素. 故得"對素數 p, 所有的同餘類對加減乘除自封,但行除法時,不能以 0 去除".

§ 3. **縮剩餘系** (reduced residue system).

前節已述及,若一類 A 中有一數與 m 互素,則 A 中所有數皆與 m 互素. 或逕述爲類 A 與 m 互素. 若類 A 與 m 互素,由定理 2.3, 吾人可定義 B/A. 特別以 A^{-1} 記 I/A. 例如:

A	0	1	2	3	4
A^{-1}	×	1	3	2	4

(mod 5)

A	0	1	2	3	4	5
A^{-1}	×	1	×	×	×	5

(mod 6)

A	0	1	2	3	4	5	6
A^{-1}	×	1	4	5	2	3	6

(mod 7)

表中"×"表示"無意義".

定義. 命 $\varphi(m)$ 爲與 m 互素之類之個數. 此 $\varphi(m)$ 名爲 Euler 函數. 在與 m 互素之諸類中各取一代表

$$a_1, \cdots, a_{\varphi(m)},$$

此名爲一縮剩餘系或簡稱縮系. 例如:

$$\varphi(1)=1,\quad \varphi(2)=1,\quad \varphi(3)=2,\quad \varphi(4)=2 \quad \text{等等}.$$

此 $\varphi(m)$ 也可述爲: 不大於 m 且與 m 互素之正整數之個數. 若 $m=p$ 爲素數,則 $\varphi(p)=p-1$.

定理 1. 若

$$a_1,\quad a_2,\cdots,\ a_{\varphi(m)}$$

爲一縮系,及 $(k,m)=1$, 則

$$ka_1,\quad ka_2,\cdots,\quad ka_{\varphi(m)}$$

亦爲一縮系.

證: 顯然有 $(ka_i,m)=1$. 故每一數代表一與 m 互素之類. 若 $ka_i\equiv ka_j$ $(\mathrm{mod}\ m)$. 因 $(k,m)=1$, 故得 $a_i\equiv a_j\ (\mathrm{mod}\ m)$. 故各數代表不同的類. 卽得定理.

定理 2 (Euler). 若 $(k,m)=1$, 則

$$k^{\varphi(m)}\equiv 1 \qquad (\mathrm{mod}\ m).$$

證: 由定理 1 易知

$$\prod_{\nu=1}^{\varphi(m)}(k\,a_\nu)\equiv\prod_{\nu=1}^{\varphi(m)}a_\nu \qquad (\mathrm{mod}\ m).$$

因 $(m,a_\nu)=1$, 故得

$$k^{\varphi(m)}\equiv 1 \qquad (\mathrm{mod}\ m).$$

取 $m=p$, 立得 Fermat 定理 (定理 1.12.4)

定理 3. 若 p 爲素數,則對所有之整數 a 有次之同餘式

$$a^p\equiv a \qquad (\mathrm{mod}\ p).$$

§4. p^2 可整除 $2^{p-1}-1$ 否? 此問題肇源頗古. 於 1828 年 Abel 曾問及有素數 p 及整數 a 使

$$a^{p-1}\equiv 1 \qquad (\mathrm{mod}\ p^2)$$

否? Jacobi 謂: 若 $p\leqslant 37$, 適合此式之解答爲

$$p=11,\qquad a=3 \text{ 或 } 9.$$

$$p=29,\qquad a=14$$

及

$$p = 37, \quad a = 18.$$

近來 Fermat 最後問題之研究,更刺激此方面之進展. 關於 Fermat 最後問題,有次之定理。

命 p 爲奇素數. 若有整數 x, y, z 使

$$x^p + y^p + z^p = 0, \quad p \nmid xyz,$$

則

$$2^{p-1} \equiv 1 \pmod{p^2} \tag{1}$$

及*

$$3^{p-1} \equiv 1 \pmod{p^2}. \tag{2}$$

是否有能同時適合 (1) 及 (2) 之素數 p 存在,尙爲一未曾解決之問題.

定義. 若

$$a^{p-1} \equiv 1 \pmod{p^2},$$

則 a 名爲 Fermat 解,不然謂之非 Fermat 解。

顯然二 Fermat 解之積仍爲一 Fermat 解. 一 Fermat 解及一非 Fermat 解之積爲一非 Fermat 解. 若分解一非 Fermat 解爲素因數積時,必有一素因數爲非 Fermat 解.

定理 1. 命 a 及 b 爲 p 之二 Fermat 解,則決不能有 q 使

$$qp = a \pm b, \quad p \nmid q.$$

證: 由定義已知

$$a^p \equiv a, \quad b^p \equiv b \pmod{p^2};$$

故

$$a^p \pm b^p \equiv a \pm b \pmod{p^2}. \tag{3}$$

若 $qp = a \pm b$, $p \nmid q$, 則

$$a^p = (\mp b + qp)^p \equiv \mp b^p \pmod{p^2}.$$

卽得

$$a^p \pm b^p \equiv 0 \pmod{p^2}.$$

以此代入 (3),得出 $a \pm b = qp \equiv 0 \pmod{p^2}$. 此乃一矛盾。

定理 2. 3 爲 11 之 Fermat 解.

---

*較近之研究,可於上結論中添入

$$n^{p-1} \equiv 1 \pmod{p^2}, \quad n = 2, 3, \cdots, 47.$$

證:

$$3^5 = 243 \equiv 1 \pmod{11^2},$$

故

$$3^{10} \equiv 1 \pmod{11^2}.$$

定理 3. 2 爲 1093 之 Fermat 解.

證: 命 $p = 1093$, 則

$$3^7 = 2187 = 2p + 1,$$

故

$$3^{14} \equiv 4p + 1 \pmod{p^2}; \tag{4}$$

又

$$2^{14} = 16384 = 15p - 11,$$

故

$$2^{28} \equiv -330p + 121 \pmod{p^2},$$
$$3^2 \cdot 2^{28} \equiv -2970p + 1089 \pmod{p^2}$$
$$\equiv -2969p - 4$$
$$\equiv 310p - 4 \pmod{p^2},$$
$$3^2 \cdot 2^{28} \cdot 7 \equiv 2170p - 28$$
$$\equiv -16p - 28 \pmod{p^2}.$$

故

$$3^2 \cdot 2^{26} \cdot 7 \equiv -4p - 7 \pmod{p^2}.$$

用二項式定理得

$$3^{14} \cdot 2^{182} \cdot 7^7 \equiv (-4p - 7)^7 \equiv -7 \cdot 4p \cdot 7^6 - 7^7 \pmod{p^2},$$

故

$$3^{14} \cdot 2^{182} \equiv -4p - 1 \pmod{p^2}. \tag{5}$$

由 (4) 及 (5) 得

$$3^{14} \cdot 2^{182} \equiv -3^{14}, \quad 2^{182} \equiv -1 \pmod{p^2},$$

故

$$2^{1092} \equiv 1 \pmod{p^2}.$$

定理 4. 3 非 1093 之 Fermat 解.

證: 若 3 爲 Fermat 解,則 3^7 亦然. 顯然, -1 爲一 Fermat 解. 因

$$3^7 - 1 = 2p,$$

故由定理 1 卽得所證.

定理 5. 小於 100 之素數,無同時適合 (1) 及 (2) 者.

證: 設 2 及 3 皆爲 Fermat 解. 則 2^l, 3^m 及 $2^l\cdot 3^m$ 亦皆爲 Fermat 解. 當然 1 也是 Fermat 解. 定理 5 可由定理 1 及以下之計算得之:

$$2=3-1,\quad 3=2+1,\quad 5=2+3,\quad 7=2^2+3,\quad 11=2+3^2,$$
$$13=2^2+3^2,\quad 17=2^3+3^2,\quad 19=2^4+3,\quad 23=-2^2+3^3,\quad 29=2+3^3,$$
$$31=2^2+3^3,\quad 37=2^6-3^3,\quad 41=2^5+3^2,\quad 43=2^4+3^3,\quad 47=2^4\cdot 3-1,$$
$$53=2\cdot 3^3-1,\ 59=2^5+3^3,\quad 61=2^6-3,\quad 67=2^6+3,\quad 71=2^3\cdot 3^2-1,$$
$$73=2^6+3^2,\quad 79=-2+3^4,\quad 83=2+3^4,\quad 89=2^3+3^4,\quad 97=2^4+3^4.$$

輓近 Lehmer 氏證明若 $p\leqslant 253,747,889$ 時,必有一不大於 47 之 m 使

$$m^{p-1}\not\equiv 1 \pmod{p^2}.$$

因之 Fermat 最後定理之一部分乃得證明.

§5. $\varphi(m)$ 之討論.

定理 1. 若 $(m, m')=1$, x 過 m 之一完全剩餘系, x' 過 m' 之一完全剩餘系,則 $mx'+m'x$ 過 mm' 之一完全剩餘系.

證: 於 mm' 個數 $mx'+m'x$ 中,若

$$mx'+m'x\equiv my'+m'y \pmod{mm'},$$

則

$$mx'\equiv my' \pmod{m'},$$
$$m'x\equiv m'y \pmod{m}.$$

由 $(m, m')=1$ 可得

$$x'\equiv y' \pmod{m'},\qquad x\equiv y \pmod{m}.$$

明所欲證.

定理 2. 若 $(m, m')=1$, x 過 m 之一縮剩餘系, x' 過 m' 之一縮剩餘系,則 $mx'+m'x$ 過 mm' 之一縮剩餘系.

證: 1) $mx'+m'x$ 與 mm' 互素. 不然,必有一素數 p 使

$$p\mid(mm',\ mx'+m'x).$$

假定 $p\mid m$, 則 $p\mid m'x$. 因 $(m, m')=1$, 故 $p\nmid m'$, 即 $p\mid x$. 即 $p\mid(m, x)$. 此不可能.

2) 凡與 mm' 互素之數 a 必與一形如

$$mx' + m'x, \quad (x, m) = (x', m') = 1$$

之數同餘 (mod mm').

由定理 1 有二整數 x 及 x' 使

$$a \equiv mx' + m'x \qquad (\mathrm{mod}\, mm').$$

今往證 $(x, m) = (x', m') = 1$. 若 $(x, m) = d \neq 1$, 則

$$(a, m) = (mx' + m'x, m) = (m'x, m) = (x, m) = d \neq 1.$$

此與原假定相背. 同法可證明 $(x', m') = 1$.

3) 於定理 1 中已證明形如 $mx' + m'x$ 之數無同餘者. 故得定理.

同時亦已證明:

定理 3. 若 $(m, m') = 1$, 則

$$\varphi(mm') = \varphi(m)\,\varphi(m').$$

卽 $\varphi(m)$ 爲一積性函數.

積性函數有一特質,祇須知素數乘方之情形,卽可推得其餘. 因若 m 之標準分解式爲

$$m = p_1^{l_1} \cdots p_s^{l_s}, \qquad p_1 < p_2 < \cdots < p_s.$$

則由定理 3 可知

$$\varphi(m) = \varphi(p_1^{l_1}) \cdots \varphi(p_s^{l_s}).$$

定理 4.

$$\varphi(p^l) = p^l\left(1 - \frac{1}{p}\right);$$

$$\varphi(m) = m \prod_{p|m}\left(1 - \frac{1}{p}\right),$$

此處 p 過 m 之不同素因子.

證: 不大於 p^l 之 p^l 個正整數中, 有 p^{l-1} 個爲 p 之倍數, 其他皆與 p 互素. 故

$$\varphi(p^l) = p^l - p^{l-1} = p^l\left(1 - \frac{1}{p}\right).$$

由此及 φ 之積性,卽得第二式.

例如: $\varphi(300) = \varphi(2^2 \cdot 3 \cdot 5^2) = 2^2 \cdot 3 \cdot 5^2\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 80.$

習題 1. 證明

$$\sum_{d|m} \varphi(d) = m,$$

式中 $\sum_{d|m}$ 表示一和,其中之變數 d 過 m 之諸因數.

習題 2. 命 P 爲 (m, n) 中不同素因數之積,則

$$\frac{\varphi(mn)}{\varphi(m)\varphi(n)} = \frac{P}{\varphi(P)}.$$

習題 3. 應用定理 1.7.1 證明定理 4.

§ 6. 同餘方程. 今往討論形如

$$ax + b \equiv 0 \pmod{m} \tag{1}$$

之方程,何時可解? 有幾個同餘類適合此方程?

解同餘方程 (1), 卽爲求方程

$$ax + b = my$$

之整解. 此種不定一次方程已於 §1.8 中討論及之. 今再複述並進一步討論如次:

若 $(a, m) = 1$, 則由定理 1.4.4, 可得 x_0, y_0 使

$$ax_0 + my_0 = 1.$$

故 $x = -bx_0$ 卽爲 (1) 式之一解. 今往證其唯一性. 若

$$ax' + b \equiv 0 \pmod{m},$$

$$ax + b \equiv 0 \pmod{m},$$

則

$$a(x - x') \equiv 0 \pmod{m}.$$

由 $(a, m) = 1$, 可得

$$x \equiv x' \pmod{m}.$$

故有唯一之同餘類適合 (1) 式. 換言之,(1) 僅有一解 x 適合 $0 \leqslant x < m$.

若 $(a, m) = d > 1$, 則 d 必整除 b, 不然無解. 如此得

$$\frac{a}{d}x + \frac{b}{d} \equiv 0 \quad \left(\bmod \frac{m}{d}\right), \quad \left(\frac{a}{d}, \frac{m}{d}\right) = 1. \tag{2}$$

由上證已知 (2) 式必有一唯一解 x_1 適合

$$0 \leqslant x_1 < \frac{m}{d}.$$

而

$$x = x_1 + \frac{m}{d} t$$

皆爲 (2) 之解，故對模 m，

$$x_1,\ x_1 + \frac{m}{d},\ x_1 + 2\frac{m}{d}, \cdots,\quad x_1 + (d-1)\frac{m}{d}$$

皆不同餘，而均適合 (1) 式．故得：

定理 1. 若 $(a, m) | b$，則(1)有 (a, m) 個互不同餘之解，mod m．不然則無解．

定理 2. 同餘方程

$$a_1 x_1 + \cdots + a_n x_n + b \equiv 0 \pmod m$$

有解 $(x_1, \cdots, x_n)$ 之必要且充分之條件爲

$$(a_1, \cdots, a_n, m) \mid b.$$

若此條件適合，則其解數（對模 m 不同餘者）爲

$$m^{n-1}(a_1, \cdots, a_n, m).$$

證：由定理 1 知此對 $n = 1$ 爲眞．今用歸納法以證之．命

$$(a_1, \cdots, a_n, m) = d$$

及

$$(a_1, \cdots, a_{n-1}, m) = d_1,$$

則

$$(d_1, a_n) = d.$$

由定理 1 知

$$a_n x_n + b \equiv 0 \pmod{d_1},\qquad 0 \leqslant x_n < m$$

有 $d \cdot \frac{m}{d_1}$ 個解．對此式之一解 x_n，命

$$\frac{a_n x_n + b}{d_1} = b_1.$$

由歸納法假定，

$$a_1 x_1 + \cdots + a_{n-1} x_{n-1} + b_1 d_1 \equiv 0 \pmod m$$

之解數爲

$$m^{n-2}(a_1, \cdots, a_{n-1}, m) = m^{n-2} d_1.$$

故總解數為

$$\frac{md}{d_1} \cdot m^{n-2} d_1 = m^{n-1} d.$$

明所欲證.

§7. 孫子定理.

定理 1. 命 m 為 m_1 及 m_2 之最小公倍數. 同餘式

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2},$$

有公解之條件為

$$(m_1, m_2) \mid (a_1 - a_2). \tag{1}$$

若 (1) 成立,則對模 m 有唯一解.

證: 1) 命 $(m_1, m_2) = d$, 若同餘式有公解,則

$$x \equiv a_1 \pmod{d},$$
$$x \equiv a_2 \pmod{d}.$$

故 $d \mid (a_1 - a_2)$.

2) 若 $d \mid (a_1 - a_2)$,則

$$x \equiv a_1 \pmod{m_1}$$

之諸解之形必為

$$x = a_1 + m_1 y.$$

以此代入第二式,得

$$a_1 + m_1 y \equiv a_2 \pmod{m_2}.$$

由上節定理 1 之證明,此式有唯一的解, mod $\frac{m_2}{d}$. 故 x 有唯一的解, mod m.

定理 2. 若 $(m_i, m_j) = 1$ $(i \neq j)$, 則

$$x \equiv a_i \pmod{m_i}, \quad 1 \leqslant i \leqslant n$$

有唯一解, mod $m_1 \cdots m_n$.

此可由定理 1 行歸納法證明之.

今述一我國古代對此問題之實際解法. 於 §1 中已述及在孫子算經中有"物不知其數"一問. 解該問題,有次之歌訣:

"三人同行七十稀,

五樹梅花廿一枝，
七子團圓正半月，
除百零五便得知."

程大位 算法統宗 (1593).

意爲: 以 70 乘用 3 除所得之餘數, 21 乘用 5 除所得之餘數, 15 乘用 7 除所得之餘數,總加之,然後以 105 之倍數加減之. 如第一節所列之問題之解式爲

$$2 \times 70 + 3 \times 21 + 2 \times 15 = 233,$$

減去 105 之二倍,得 23. 此乃所求之數.

此法較上述之理論易於佈算. 果何術而致之? 70, 21, 15 之來源又如何? 玆答覆如次: 70 者乃 5,7 之倍數,而 3 除餘 1 之數. 21 乃 3,7 之倍數, 5 除餘 1 之數. 15 乃 3,5 之倍數, 7 除餘 1 之數. 故

$$70a + 21b + 15c$$

顯然 3 除餘 a, 5 除餘 b, 而 7 除餘 c.

進而論 70, 21, 15 之根源. 卽如何求出 x 使

$$x \equiv 0 \pmod{m_1}, \quad x \equiv 0 \pmod{m_2}, \quad x \equiv 1 \pmod{m_3}$$

此處 $(m_1, m_2) = (m_2, m_3) = (m_3\ m_1) = 1$? 卽如何求 $x = m_1m_2y$ 之 y 使

$$m_1m_2y \equiv 1 \pmod{m_3}.$$

由輾轉相除法,易得 y 及 z 使

$$m_1m_2y - m_3z = 1.$$

故 m_1m_2y 卽爲所求之數.

習題 1. 換 3, 5, 7 爲 3, 7, 11 以求與 70, 21, 15 所對應之數.

習題 2. 七數剩一,八數剩二,九數剩三,問本數.

習題 3. 十一數餘三,十二數餘二,十三數餘一,問本數.

習題 4. 二數餘一,五數餘二,七數餘三,九數餘四,問本數.

(以上三題見楊輝續古摘奇算法 (1275)).

習題 5. 今有數不知總,以五累減之無賸,以七百十五累減之賸十,以二百四十七累減之賸一百四十,以三百九十一累減之賸二百四十五,以一百八十七累減之賸一百零九. 問總數若干.

(答: 1,0020)

黃宗憲求一術通解.

註: "物不知其數" 又名 "鬼谷算", "秦王暗點兵", "剪管術", "隔牆算" "神奇妙算", "大衍求一術" 等等.

§ 8. 高次同餘式. m 爲一固定之自然數. $f(x)$ 爲一整係數多項式

$$f(x) = a_n x^n + \cdots + a_0.$$

玆論同餘方程

$$f(x) \equiv 0 \pmod{m}. \tag{1}$$

若 x_0 爲其一解, 則 $x_0 + mt$ 均爲其解. 卽若 x_0 適合此式, 則 x_0 所代表之剩餘類中之每一數皆適合此式. 故此式之解數云者乃非同餘之解之個數之義, 而爲不同剩餘類適合 (1) 式之個數.

高次同餘方程之解數, 非常不規則, 例如:

1. 同餘方程

$$x^3 - x = (x-1)x(x+1) \equiv 0 \pmod{6}$$

有六個解.

2. 同餘方程

$$x^2 + 1 \equiv 0 \pmod{3}$$

無解.

3. 同餘方程

$$(x-1)(x-p-1) \equiv 0 \pmod{p^2}$$

之解爲 $1, p+1, 2p+1, \cdots, (p-1)p+1$. 總共有 p 個.

故解法至爲困難複雜, 但有次之定理, 不無相助處.

定理 1. 若 $(m_1, m_2) = 1$, 則同餘方程

$$f(x) \equiv 0 \pmod{m_1 m_2} \tag{2}$$

之解數爲二方程

$$f(x) \equiv 0 \pmod{m_1}, \tag{3}$$

$$f(x) \equiv 0 \pmod{m_2}, \tag{4}$$

之解數之積. 命

$$m = m_1 m_2 = p_1^{l_1} \cdots p_s^{l_s} \quad (p_1 < p_2 < \cdots < p_s)$$

爲 m 之標準分解式. 用上之理立得 (2) 之解數爲

$$f(x)\equiv 0 \pmod{p_i^{l_i}}, \qquad 1\leqslant i\leqslant s$$

之解數之積.

證: 顯然 (2) 之解答適合 (3) 及 (4) 兩式.

反之,命 c_1 爲 (3) 之解, c_2 爲 (4) 之解. 命 c 爲

$$c\equiv c_1 \pmod{m_1}, \qquad c\equiv c_2 \pmod{m_2}$$

之解. 由孫子定理,此 c 存在,且對模 m 唯一. 此 c 適合 (2) 式,因由

$$m_1\mid f(c), \qquad m_2\mid f(c)$$

而得 $m|f(c)$ 故也.

§ 9. 素數乘方爲模之高次同餘方程.

定理 1. 命 p 爲素數. 同餘方程

$$f(x)=a_n x^n+\cdots+a_0\equiv 0 \pmod{p} \tag{1}$$

之解數 $\leqslant n$, 重解計算在內.

證: 可假定 $p\nmid a_n$. 若 (1) 無解, 則定理爲眞. 若 a 爲其一解, 則可書

$$f(x)=(x-a)f_1(x)+r_1.$$

以 a 代入此式,顯見 $p|r_1$. 故

$$f(x)\equiv(x-a)f_1(x) \pmod{p}.$$

若 a 又爲 $f_1(x)\equiv 0 \pmod{p}$ 之解,則同樣可得

$$f_1(x)\equiv(x-a)f_2(x) \pmod{p}.$$

此時我們稱 a 爲 $f(x)\equiv 0 \pmod{p}$ 之重解. 若

$$f(x)\equiv(x-a)^h g_1(x) \pmod{p},$$

$g_1(a)\not\equiv 0 \pmod{p}$, 則稱 a 爲 $f(x)\equiv 0 \pmod{p}$ 之 h 重解. 由我們的證明容易看出 $g_1(x)$ 之次數是 $n-h$.

設另有一解 b, 則

$$0\equiv f(b)\equiv(b-a)^h g_1(b) \pmod{p}.$$

因爲 $p\nmid(b-a)$, 故

$$g_1(b)\equiv 0 \pmod{p}.$$

若 b 爲 $g_1(x)$ 之 k 重解,則同樣有

$$f(x) \equiv (x-a)^h (x-b)^k g_2(x) \pmod{p}.$$

如是繼續進行,可得

$$f(x) \equiv (x-a)^h (x-b)^k \cdots (x-c)^l g(x) \pmod{p}.$$

$g(x)$ 之次數等於 $n-h-k-\cdots-l$, 且

$$g(x) \equiv 0 \pmod{p}$$

不再有解. 我們的定理卽已證明.

因爲同餘方程

$$x^{p-1} \equiv 1 \pmod{p}$$

以 $1, 2, \cdots, p-1$ 爲解,故

$$x^{p-1}-1 \equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod{p}. \qquad (2)$$

以 $x=0$ 代入此式立得:

定理 2 (Wilson). 若 p 爲素數,則

$$(p-1)! \equiv -1 \pmod{p}.$$

若 $p \neq 2$, 則右邊有 $p-1$ 個負號,而 $p-1$ 爲偶數,故由 (2) 直接得出. 若 $p=2$, 則定理 2 顯然眞確.

定理 3. 命

$$f'(x) = n a_n x^{n-1} + \cdots + 2a_2 x + a_1.$$

若 $f(x) \equiv 0$, $f'(x) \equiv 0 \pmod{p}$ 無公解,則

$$f(x) \equiv 0 \pmod{p^l}$$

之解數等於

$$f(x) \equiv 0 \pmod{p}$$

之解數.

證: 此可由歸納法證之. 當 $l=1$ 自不必證. 命 x_1 爲

$$f(x) \equiv 0 \pmod{p^{l-1}}$$

之一解,則

$$f(x_1 + p^{l-1} y) \equiv f(x_1) + p^{l-1} y f'(x_1) \pmod{p^l}$$

(因 $(x+p^{l-1}y)^n \equiv x^n + np^{l-1}yx^{n-1} \pmod{p^l}$ 故也). 但 $p \nmid f'(x_1)$, 故有唯一之 y, 使

$$f(x_1 + p^{l-1} y) \equiv 0 \pmod{p^l}.$$

定理 4. 同餘方程

$$x^{p-1}\equiv 1 \pmod{p^l}$$

有 $p-1$ 個解.

此定理可由定理 3 直接得之.

§ 10. Wolstenholme 定理.

定理 1. 命 p 爲素數 >3. 以 $\frac{1}{s}$ 表一整數 s^* 使

$$s\, s^*\equiv 1 \pmod{p^2}$$

者,則

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}\equiv 0 \pmod{p^2}.$$

證: 命

$$(x-1)(x-2)\cdots(x-(p-1))=x^{p-1}-s_1x^{p-2}+\cdots+s_{p-1}, \tag{1}$$

則

$$s_{p-1}=(p-1)!$$

因

$$(x-1)(x-2)\cdots(x-(p-1))\equiv x^{p-1}-1 \pmod{p}, \tag{2}$$

故

$$p\mid (s_1,\cdots,s_{p-2}). \tag{3}$$

於 (1) 中命 $x=p$, 則

$$(p-1)!=p^{p-1}-s_1p^{p-2}+\cdots-s_{p-2}p+s_{p-1},$$

卽

$$p^{p-2}-s_1p^{p-3}+\cdots+s_{p-3}p-s_{p-2}=0.$$

若 $p>3$, 則由 (3) 式得

$$s_{p-2}\equiv 0 \pmod{p^2},$$

卽

$$p^2\mid (p-1)!\left(1+\frac{1}{2}+\cdots+\frac{1}{p-1}\right),$$

亦卽

$$1^*+2^*+\cdots+(p-1)^*\equiv 0 \pmod{p^2}.$$

明所欲證.

第　三　章

二　次　剩　餘

§1. 定義及 Euler 判別條件.

定義 1. 設 m 爲大於 1 之整數. 假定 $(m, n) = 1$, 若

$$x^2 \equiv n \qquad (\text{mod } m)$$

可解，則 n 謂之對模 m 之二次剩餘，或二次剩餘，mod m. 不然則謂之對模 m 之二次非剩餘.

今將對 m 互素之整數分爲二類：一類爲二次剩餘，一類爲二次非剩餘.

例. 1, 2, 4 爲 7 之二次剩餘; 3, 5, 6 爲二次非剩餘.

定義 2 (Legendre 符號). 設 p 爲大於 2 之素數. $p \nmid n$. 命

$$\left(\frac{n}{p}\right) = \begin{cases} 1, & \text{若 } n \text{ 爲二次剩餘, mod } p, \\ -1, & \text{若 } n \text{ 爲二次非剩餘, mod } p. \end{cases}$$

此符號顯然有次之性質：若 $n \equiv n' (\text{mod } p)$ 及 $p \nmid n$, 則

$$\left(\frac{n}{p}\right) = \left(\frac{n'}{p}\right).$$

定理 1. 命 $p > 2$. 於一縮系 (mod p) 中，有 $\frac{1}{2}(p-1)$ 個二次剩餘，有 $\frac{1}{2}(p-1)$ 個二次非剩餘，且

$$1^2, \cdots, \left(\frac{1}{2}(p-1)\right)^2$$

卽爲其諸二次剩餘，mod p.

證：若

$$x^2 \equiv n \qquad (\text{mod } p) \tag{1}$$

有解，則至多有二解. 由

$$(p-x)^2 \equiv (-x)^2 = x^2 \equiv n \qquad (\text{mod } p),$$

可知 (1) 式必有一根適合

$$1 \leqslant x \leqslant \frac{1}{2}(p-1). \tag{2}$$

卽若 (1) 有解,必有一解適合 (2).

又

$$1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2$$

間無同餘者. 因

$$a^2 - b^2 = (a-b)(a+b)$$

之二因子皆小於 p 而不能爲 p 之倍數也. 故得定理.

定理 2 (Euler 之判別條件). 設 p 是一奇素數,則

$$n^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right) \pmod p.$$

證: 1) 若

$$\left(\frac{n}{p}\right) = 1,$$

則有一 x 使

$$x^2 \equiv n \pmod p,$$

卽

$$n^{\frac{1}{2}(p-1)} \equiv x^{p-1} \equiv 1 \pmod p.$$

2) 由定理 2.9.1 已知

$$n^{\frac{1}{2}(p-1)} \equiv 1 \pmod p$$

之解數 $\leqslant \frac{1}{2}(p-1)$. 與 1) 相結合,此式當有 $\frac{1}{2}(p-1)$ 個解,卽爲諸二次剩餘, mod p, 而無他.

3) 又有

$$p \mid (n^{p-1}-1) = (n^{\frac{1}{2}(p-1)}-1)(n^{\frac{1}{2}(p-1)}+1).$$

故若 $p \nmid (n^{\frac{1}{2}(p-1)}-1)$,則

$$n^{\frac{1}{2}(p-1)} + 1 \equiv 0 \pmod p.$$

定理於是證明.

由此定理立得:

定理 3. 若 $p \nmid mn$, 則

$$\left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = \left(\frac{mn}{p}\right).$$

即$\left(\frac{m}{p}\right)$爲一積性函數.

由此立得:

定理 4. 1) 二二次剩餘之積仍爲二次剩餘, mod p;

2) 二二次非剩餘之積爲二次剩餘, mod p;

3) 一二次剩餘與一二次非剩餘之積爲一二次非剩餘, mod p.

§ 2. 計算法則.

由定理 1.3 可知任一 Legendre 符號之算出,祇有賴於

$$\left(\frac{-1}{p}\right),\ \left(\frac{2}{p}\right),\ \left(\frac{q}{p}\right) \qquad (q\text{ 爲一奇素數})$$

之值而已. 蓋若任與一數

$$n = \pm 2^m \cdot q_1^{l_1} \cdots q_s^{l_s}, \qquad 2 < q_1 < \cdots < q_s,$$

則

$$\left(\frac{n}{p}\right)=\left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^m\left(\frac{q_1}{p}\right)^{l_1}\cdots\left(\frac{q_s}{p}\right)^{l_s}.$$

於定理 1.2 中取 $n=-1$, 則得

$$\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}} \qquad (\text{mod}\, p).$$

但兩邊之值皆祇能爲 ± 1, 故得

定理 1. 若 $p>2$, 則$\left(\frac{-1}{p}\right)=(-1)^{\frac{1}{2}(p-1)}$.

換言之, 若 $p\equiv 1 \pmod 4$, 則 -1 爲二次剩餘, mod p, 而若 $p\equiv 3 \pmod 4$,則 -1 非二次剩餘, mod p.

由此可知 x^2+1 之奇素數因子必$\equiv 1 \pmod 4$.

定理 2 (Gauss 引). 命 $p>2$, $p\nmid n$. 設$\frac{1}{2}(p-1)$ 個數

$$n,\ 2n,\ \cdots,\ \frac{1}{2}(p-1)\,n \qquad (\text{mod}\, p)$$

之最小正餘數中有 m 個大於 $\frac{1}{2}p$,則

$$\left(\frac{n}{p}\right)=(-1)^m.$$

例 1. $p=7$, $n=10$, 則

$$10, 20, 30 \equiv 3, 6, 2 \qquad (\bmod 7),$$

其中有一個 $> \frac{7}{2}$. 故 $m=1$, 而得 $\left(\frac{10}{7}\right) = -1$.

例 2. $p=11$, $n=2$, 則

$$2, 4, 6, 8, 10 \qquad (\bmod 11)$$

中大於 $\frac{11}{2}$ 者有三個. 故 $\left(\frac{2}{11}\right) = -1$.

證: 以

$a_1, \cdots, a_l$ $(l = \frac{1}{2}(p-1) - m)$ 表諸餘數之小於 $\frac{1}{2}p$ 者;

$b_1, \cdots, b_m$ 表諸餘數之大於 $\frac{1}{2}p$ 者,

則

$$\prod_{s=1}^{l} a_s \prod_{t=1}^{m} b_t \equiv \prod_{k=1}^{\frac{1}{2}(p-1)} kn = \left(\frac{p-1}{2}\right)!\, n^{\frac{p-1}{2}} \qquad (\bmod p). \tag{1}$$

$p - b_t$ 亦在 1 及 $\frac{1}{2}(p-1)$ 之間,故 a_s 及 $p - b_t$ 爲在 1 及 $\frac{1}{2}(p-1)$ 之間的 $\frac{1}{2}(p-1)$ 個數. 今往證其各不相同,祇須證明

$$a_s \neq p - b_t$$

卽足. 若 $a_s + b_t = p$, 則有 x 及 y 使

$$xn + yn \equiv 0 \ (\bmod p), \qquad 1 \leqslant x \leqslant \frac{1}{2}(p-1), \qquad 1 \leqslant y \leqslant \frac{1}{2}(p-1),$$

卽

$$x + y \equiv 0 \qquad (\bmod p).$$

此不可能. 故

$$\prod_{s=1}^{l} a_s \prod_{t=1}^{m} (p - b_t) = \left(\frac{p-1}{2}\right)!.$$

而此式之左端 (由 (1) 式)

$$\equiv (-1)^m \prod_{s=1}^{l} a_s \prod_{t=1}^{m} b_t \equiv (-1)^m n^{\frac{1}{2}(p-1)} \left(\frac{p-1}{2}\right)! \qquad (\bmod p).$$

故得

$$n^{\frac{1}{2}(p-1)} \equiv (-1)^m \qquad (\bmod p).$$

由 Euler 判別條件可知

$$\left(\frac{n}{p}\right)\equiv(-1)^m \qquad (\bmod p).$$

立得

$$\left(\frac{n}{p}\right)=(-1)^m.$$

於此定理（定理 2）中取 $n=2$，則

$$2,\ 2\cdot2,\ 2\cdot3,\ \cdots,\ \frac{1}{2}(p-1)\cdot2$$

已在 0 與 p 之間．今往算出適合

$$\frac{p}{2}<2k<p \qquad 即 \qquad \frac{p}{4}<k<\frac{p}{2}$$

之 k 之個數．即得 $m=\left[\frac{p}{2}\right]-\left[\frac{p}{4}\right]$.

命 $p=8a+r,\ r=1,3,5,7$，則得

$$m=2a+\left[\frac{r}{2}\right]-\left[\frac{r}{4}\right]\equiv0,1,1,0 \qquad (\bmod 2).$$

故得：

定理 3. 若 $p>2$，則

$$\left(\frac{2}{p}\right)=(-1)^{\frac{1}{8}(p^2-1)}.$$

換言之，若 $p\equiv\pm1$, (mod 8)，則 2 爲二次剩餘，mod p；若 $p\equiv\pm3$ (mod 8)，則 2 爲二次非剩餘，mod p.

立得 x^2-2 之奇素數因子必 $\equiv\pm1$ (mod 8).

習題．若 $n>0$, $4n+3$, $8n+7$ 皆爲素數，$2^{4n+3}-1=M_{4n+3}$ 非素數．由此證明以下的關於 Mersenne 數之性質：

$$23|M_{11},\quad 47|M_{23},\quad 167|M_{83},\quad 263|M_{131},$$
$$359|M_{179},\quad 383|M_{191},\quad 479|M_{239},\quad 503|M_{251}.$$

§3. 互逆定律．

定理 1. 命 $p>2,\ q>2$ 爲二素數，且 $p\neq q$，則

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}.$$

換言之，若 $p\equiv q\equiv3$ (mod 4)，則二同餘式

$$x^2 \equiv p \pmod{q}, \qquad x^2 \equiv q \pmod{p}$$

中一可解,一不可解. 不然,則皆可解,或皆不可解.

此乃初等數論中最著名且重要之 Gauss 氏互逆定理 (Law of reciprocity). Gauss 稱此爲 Legendre 之互逆定理. 但 Legendre 雖發現此定理而未能確切證明之. 此定理 Gauss 稱之謂"數論之酵母". 後來 Kummer, Eisenstein, Hilbert, Artin, Furtwängler 等之代數數論之研究,證明此說,實深且切也. Gauss 氏之深湛研究,曾作原則方面大相逕庭之證明,由此而發生之研究實難於列舉.

證: 今暫不除外 $q=2$ 之情形,祇假定 $p \neq q$ 且皆爲素數. 當 $1 \leqslant k \leqslant \leqslant \frac{1}{2}(p-1)$,可書

$$kq = q_k p + r_k, \qquad q_k = \left[\frac{kq}{p}\right], \qquad 1 \leqslant r_k \leqslant p-1.$$

命

$$a = \sum_{s=1}^{l} a_s, \quad b = \sum_{t=1}^{m} b_t$$

(此處 a_s 及 b_t 之意義見上節). 則得

$$\sum_{k=1}^{\frac{1}{2}(p-1)} r_k = a + b. \tag{1}$$

由上節定理之證明已知 a_s, $p - b_t$ 與 $1, 2, \cdots, \frac{1}{2}(p-1)$ 諸數相同. 卽得

$$\frac{p^2-1}{8} = 1 + 2 + \cdots + \frac{1}{2}(p-1) = a + mp - b. \tag{2}$$

又

$$\frac{p^2-1}{8}q = \sum_{k=1}^{\frac{1}{2}(p-1)} kq = p\sum_{k=1}^{\frac{1}{2}(p-1)} q_k + \sum_{k=1}^{\frac{1}{2}(p-1)} r_k = p\sum_{k=1}^{\frac{1}{2}(p-1)} q_k + a + b. \tag{3}$$

(3) 減 (2),立得

$$\frac{p^2-1}{8}(q-1) = p\sum_{k=1}^{\frac{1}{2}(p-1)} q_k - mp + 2b,$$

卽

$$\frac{p^2-1}{8}(q-1) \equiv \sum_{k=1}^{\frac{1}{2}(p-1)} q_k - m \pmod{2}. \tag{4}$$

1) (定理 2.3 之另證). 取 $q=2$, 則 q_k 皆爲 0, 故

$$\frac{p^2-1}{8} \equiv -m \qquad (\bmod 2)\,.$$

2) 設 $q>2$, 則

$$m \equiv \sum_{k=1}^{\frac{1}{2}(p-1)} q_k \qquad (\bmod 2)\,.$$

故

$$\left(\frac{q}{p}\right)=(-1)^m=(-1)^{\sum_{k=1}^{\frac{1}{2}(p-1)} q_k}=(-1)^{\sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{kq}{p}\right]}.$$

同法

$$\left(\frac{p}{q}\right)=(-1)^{\sum_{l=1}^{\frac{1}{2}(q-1)}\left[\frac{lp}{q}\right]},$$

卽得

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{kq}{p}\right]+\sum_{l=1}^{\frac{1}{2}(q-1)}\left[\frac{lp}{q}\right]}.$$

若能證明

$$\sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{kq}{p}\right]+\sum_{l=1}^{\frac{1}{2}(q-1)}\left[\frac{lp}{q}\right]=\frac{p-1}{2}\,\frac{q-1}{2} \quad 或 \equiv \frac{p-1}{2}\,\frac{q-1}{2} \quad (\bmod 2),$$

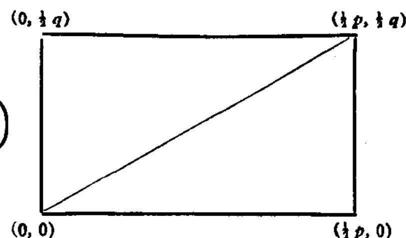
則此定理已明. 此卽下引:

引.

$$\sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{kq}{p}\right]+\sum_{l=1}^{\frac{1}{2}(q-1)}\left[\frac{lp}{q}\right]=\frac{p-1}{2}\,\frac{q-1}{2}.$$

證: 作長方形以

$$(0,0),\left(0,\frac{1}{2}q\right),\left(\frac{1}{2}p,\ 0\right),\left(\frac{1}{2}p,\ \frac{1}{2}q\right)$$



爲頂點者,經原點之對角線上無整點(整點卽爲二坐標皆爲整數之點). 因若此對角線上有整點 (x, y), 則

$$xq-yp=0\,.$$

卽得 $p|x$, $q|y$. 而此種之點在長方形之外. 長方形中之整點總數爲 $\frac{p-1}{2}\frac{q-1}{2}$. 對角線下之三角形中之整點數爲

$$\sum_{k=1}^{\frac{1}{2}(p-1)}\left[\frac{kq}{p}\right],$$

而其上之三角形中之整點數爲

$$\sum_{l=1}^{\frac{1}{2}(q-1)}\left[\frac{lp}{q}\right].$$

故得此引.

例 1. 求以 3 爲二次剩餘之素數 $p\,(>3)$.

由互逆定理,

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}.$$

因

$$\left(\frac{p}{3}\right)=\begin{cases}\left(\frac{1}{3}\right)=1, & \text{若 } p\equiv 1 \pmod 3,\\ \left(\frac{-1}{3}\right)=-1, & \text{若 } p\equiv 2 \pmod 3;\end{cases}$$

$$(-1)^{\frac{p-1}{2}}=\begin{cases}1, & \text{若 } p\equiv 1 \pmod 4,\\ -1, & \text{若 } p\equiv -1 \pmod 4.\end{cases}$$

故由孫子定理可以算出

$$\left(\frac{3}{p}\right)=\begin{cases}1, & \text{若 } p\equiv \pm 1 \pmod{12},\\ -1, & \text{若 } p\equiv \pm 5 \pmod{12}.\end{cases}$$

例 2. 求以 5 爲二次剩餘之素數 $p(\neq 5)$.

由互逆定理 $\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right)$ 及

$$\left(\frac{1}{5}\right)=1,\ \left(\frac{2}{5}\right)=(-1)^{\frac{5^2-1}{8}}=-1,\ \left(\frac{3}{5}\right)=\left(\frac{-2}{5}\right)=-1,\ \left(\frac{4}{5}\right)=1,$$

可知

$$\left(\frac{5}{p}\right)=\begin{cases}1, & \text{若 } p\equiv \pm 1 \pmod 5,\\ -1, & \text{若 } p\equiv \pm 2 \pmod 5.\end{cases}$$

例 3. 求以 10 爲二次剩餘之素數 p.

由例 2 及孫子定理可以算出:

$$\left(\frac{10}{p}\right)=\begin{cases}+1, & 若\ p\equiv\pm1,\pm3,\pm9,\pm13 \pmod{40},\\ -1, & 若\ p\equiv\pm7,\pm11,\pm17,\pm19 \pmod{40}.\end{cases}$$

例 4. 同餘式

$$x^2\equiv-1457 \pmod{2389}$$

可解否? 此 2389 是素數,以 p 表之.

因 $-1457=-31\times47$, 故由

$$\left(\frac{-1}{p}\right)=1,\left(\frac{31}{p}\right)=\left(\frac{p}{31}\right)=\left(\frac{2}{31}\right)=1,$$

$$\left(\frac{47}{p}\right)=\left(\frac{p}{47}\right)=\left(\frac{3}{47}\right)\left(\frac{13}{47}\right)=-\left(\frac{47}{3}\right)\left(\frac{47}{13}\right)=$$

$$=-\left(\frac{2}{3}\right)\left(\frac{8}{13}\right)=-\left(\frac{2}{3}\right)\left(\frac{2}{13}\right)=-1,$$

可知 $\left(\frac{-1457}{2389}\right)=-1$, 即該同餘式不可解.

習題 1. 證 $\left(\frac{3}{73}\right)=1$, $\left(\frac{17}{73}\right)=-1$.

習題 2. 證 $\left(\frac{195}{1901}\right)=-1$, $\left(\frac{74}{101}\right)=-1$, $\left(\frac{365}{1847}\right)=1$.

習題 3. 若 $p\equiv\pm1$ 或 $\pm5 \pmod{24}$, 則 $\left(\frac{6}{p}\right)=1$;

若 $p\equiv\pm7$ 或 $\pm11 \pmod{24}$, 則 $\left(\frac{6}{p}\right)=-1$.

§4. 實際算法. 以上之理論,簡誠簡矣,美誠美矣,但其實際效用僅在負方. 何以言之? 若由此種判別法,知該同餘式不可解,則問題已解決,但若該式可解,進而問如何解出,則茫然無緒. 切實言之,當 p 大時,實際算出

$$x^2\equiv n \pmod{p}$$

之解,誠非易事. 但若 $p\equiv3 \pmod 4$ 或 $p\equiv5 \pmod 8$, 吾人有次之方法:

1) $p\equiv3 \pmod 4$. 因 $\left(\frac{n}{p}\right)=1$, 故

$$n^{\frac{1}{2}(p-1)}\equiv1 \pmod{p},$$

即

$$(n^{\frac{1}{4}(p+1)})^2\equiv n \pmod{p},$$

即 $n^{\frac{1}{4}(p+1)}$ 爲所求之解答.

2) $p\equiv 5 \pmod 8$. 先求 $n=-1$ 時之解答. 由 Wilson 定理

$$-1\equiv (p-1)!\equiv 1\cdot 2\cdots\left(\frac{p-1}{2}\right)\cdot\left(p-\left(\frac{p-1}{2}\right)\right)\cdots(p-2)(p-1) \pmod p \quad (1)$$

$$\equiv\left(1\cdot 2\cdots\frac{1}{2}(p-1)\right)^2\equiv\left(\left(\frac{1}{2}(p-1)\right)!\right)^2 \pmod p.$$

故解出所需. 因 $\left(\frac{n}{p}\right)=1$, 故

$$n^{\frac{1}{2}(p-1)}-1\equiv 0 \pmod p.$$

n 適合

$$n^{\frac{1}{4}(p-1)}\equiv 1 \pmod p$$

或

$$n^{\frac{1}{4}(p-1)}\equiv -1 \pmod p.$$

由前式可知

$$n^{\frac{1}{4}(p+3)}\equiv (n^{\frac{1}{8}(p+3)})^2\equiv n \pmod p.$$

由後式,則

$$(n^{\frac{1}{8}(p+3)})^2\equiv -n \pmod p,$$

而

$$\left(n^{\frac{1}{8}(p+3)}\left(\frac{p-1}{2}\right)!\right)^2\equiv n \pmod p.$$

3) $p\equiv 1 \pmod 8$. 此乃較難之情況.

當 p 不太大時,通常用間接法以解之,卽用逐步捨棄之方法: 解同餘式

$$x^2\equiv n \pmod p$$

與解不定方程

$$x^2=n+py$$

相同. 吾人可加一無關緊要之條件 $0<n<p$. 設 x 爲正且 $<\frac{1}{2}p$, 則 $x^2<\frac{1}{4}p^2$. 如此則 $0<y<\frac{1}{4}p$. 固已捨棄一大部分矣. 取 e 與 p 互素, 且 >2. 求其二次非剩餘 $n_1, n_2, n_3\cdots$ 等,且以 $v_1, v_2, \cdots$ 表

$$n+py\equiv n_1,\quad n+py\equiv n_2,\cdots \pmod e$$

之解. 若 $y\equiv v_i \pmod e$, 則 $py+n$ 爲 e 之二次非剩餘, 故非平方數. 故能捨棄諸 $y\equiv v_i \pmod e$ 者,取不同之 e 逐步捨棄. 待數目較小,計算不太麻煩時,直接代入試驗得之.

例. 解

$$x^2 \equiv 73 \pmod{127}.$$

今往解不定方程

$$x^2 = 127y + 73,$$

此 y 在 1 至 31 $\left(=\left[\frac{127}{4}\right]\right)$ 之間.

取 $e=3$, $n_1=2$,

$$73 + 127y \equiv 2 \pmod{3},$$

則 $y \equiv 1 \pmod{3}$. 玆遺留下:

2, 3, 5, 6, 8, 9, 11, 12, 14, 15, 17, 18, 20, 21, 23, 24, 26, 27, 29, 30.

再取 $e=5$, $n_1=2$, $n_2=3$, 由同餘式

$$127y + 73 \equiv 2, 3 \pmod{5},$$

得出 $v_1 \equiv 2$, $v_2 \equiv 0 \pmod{5}$, 今遺留下:

3, 6, 8, 9, 11, 14, 18, 21, 23, 24, 26, 29.

再取 $e=7$, $n_1=3$, $n_2=5$, $n_3=6$. 由同餘式

$$127y + 73 \equiv 3, 5, 6 \pmod{7},$$

卽

$$y + 3 \equiv 3, 5, 6 \pmod{7},$$

$$y \equiv 0, 2, 3 \pmod{7}.$$

今祗遺留

6, 8, 11, 18, 26, 29

六數而已. 代入試驗, 由

$$73 + 8 \times 127 = 1089 = 33^2,$$

故該式之解為

$$x \equiv \pm 33 \pmod{127}.$$

注意: 於試驗時, 如已試 e 及 e', 則不必試 ee'. 若已試奇數之 e, 則 $2e$ 亦不必再試.

以上所述皆與 Gauss 有關, 故此"數學王子", 不特"老謀"抑且"深算"也.

§5. 二次同餘式之根數.

定理 1. 命 $l>0$, $p \nmid n$. 若 $p>2$, 則同餘式

$$x^2 \equiv n \qquad (\bmod p^l)$$

之解數爲 $1+\left(\frac{n}{p}\right)$.

若 $p=2$, 則分三種情况論列之:

1) $l=1$, 則有一根;

2) $l=2$, 視 $n\equiv 1$ 或 $3 \pmod 4$,該式有二根或無根;

3) $l>2$, 視 $n\equiv 1$ 或 $\not\equiv 1 \pmod 8$, 該式有四根或無根.

證: 先討論 $p=2$ 之情况:

1) 此爲顯然;

2) $x^2\equiv 3 \pmod 4$ 無解, $x^2\equiv 1 \pmod 4$ 有二解 $\pm 1 \pmod 4$, 故亦毋待詳論;

3) 若該式可解, 則 x 必爲奇數, 命之爲 $2k+1$. 因

$$(2k+1)^2 = 4k(k+1)+1 = 8\cdot\frac{k(k+1)}{2}+1\equiv 1 \qquad (\bmod 8).$$

故若 $n\not\equiv 1 \pmod 8$, 該式不能有解.

今設 $n\equiv 1 \pmod 8$,當 $l=3$, 顯有四根: 1, 3, 5, 7. 當 $l>3$, 用歸納法證之: 命 a 適合 $a^2\equiv n \pmod{2^{l-1}}$, 則

$$(a+2^{l-2}b)^2\equiv a^2+2^{l-1}b \qquad (\bmod 2^l).$$

取 $b=\frac{n-a^2}{2^{l-1}}$, 則 $a+2^{l-2}b$ 乃對模 2^l 之一解. 故 $x^2\equiv n \pmod{2^l}$ 必有解存在, 設 x_1 爲其一解, x_2 爲任意解, 則 $x_1^2-x_2^2\equiv(x_1-x_2)(x_1+x_2)\equiv 0 \pmod{2^l}$,因 x_1-x_2, x_1+x_2 皆爲偶數,故 $\frac{x_1-x_2}{2}\cdot\frac{x_1+x_2}{2}\equiv 0 \pmod{2^{l-2}}$,但 $\frac{x_1-x_2}{2}$, $\frac{x_1+x_2}{2}$ 不能同時爲奇數,或同時爲偶數,否則其和 x_1 不能爲奇數,故必 $x_1\equiv x_2 \pmod{2^{l-1}}$ 或 $x_1\equiv -x_2 \pmod{2^{l-1}}$, 即 $x_2=\pm x_1+k2^{l-1}$ ($k=0$ 或 1), 即 $x^2\equiv n \pmod{2^l}$ 至多有四解, 但 $\pm x_1$, $\pm x_1+2^{l-1}$ 確爲其不相同餘之四解,故此方程恰有四解.

當 $p>2$, 而 $l=1$, 此結果顯然,更由定理 2.9.3 得出本定理之全部.

由第二章之結果, 吾人可以算出以任一整數 m 爲模之二次同餘式之解數.

§ 6. Jacobi 符號. 本節中常設 m 爲正奇數.

定義. 命 m 之標準分解式爲

$$m=\prod_{r=1}^{t}p_r,$$

其中 p_r 准許重複. 若 $(n, m)=1$, 則定義

$$\left(\frac{n}{m}\right)=\prod_{r=1}^{t}\left(\frac{n}{p_r}\right).$$

此乃 Jacobi 符號.

例如: $\left(\frac{1}{m}\right)=1$. 若 $(a, m)=1$, 則 $\left(\frac{a^2}{m}\right)=1$.

請特別注意: 若 $\left(\frac{n}{m}\right)=1$, 並不說明同餘式

$$x^2\equiv n \pmod m$$

爲可解.

極易得出此項符號之運算法則:

定理 1 (**計算法則**). 設 m 與 m' 爲正奇數.

(i) 若 $n\equiv n' \pmod m$ 及 $(n, m)=1$,

則

$$\left(\frac{n}{m}\right)=\left(\frac{n'}{m}\right).$$

(ii) 若 $(n, m)=(n, m')=1$, 則

$$\left(\frac{n}{m}\right)\left(\frac{n}{m'}\right)=\left(\frac{n}{mm'}\right).$$

(iii) 若 $(n, m)=(n', m)=1$, 則

$$\left(\frac{n}{m}\right)\left(\frac{n'}{m}\right)=\left(\frac{nn'}{m}\right).$$

定理 2. $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$.

證: 祇須證明

$$\sum_{i=1}^{t}\frac{p_i-1}{2}\equiv\frac{\prod_{i=1}^{t}p_i-1}{2} \pmod 2$$

卽足. 此當 $t=1$ 時顯然無誤. 又對任二奇數 u 及 v 常有

$$\frac{u-1}{2}+\frac{v-1}{2}\equiv\frac{uv-1}{2} \pmod 2 \quad (\text{卽 } (u-1)(v-1)\equiv 0 \pmod 4). \tag{1}$$

故用歸納法

$$\sum_{i=1}^{t}\frac{p_i-1}{2}\equiv\sum_{i=1}^{t-1}\frac{p_i-1}{2}+\frac{p_t-1}{2}\equiv$$

$$\equiv\frac{\prod_{i=1}^{t-1}p_i-1}{2}+\frac{p_t-1}{2}\equiv\frac{\prod_{i=1}^{t}p_i-1}{2}\qquad(\mathrm{mod}\ 2).$$

卽得定理.

定理 3.

$$\left(\frac{2}{m}\right)=(-1)^{\frac{1}{8}(m^2-1)}.$$

證: 與上同法,唯將 (1) 換爲

$$\frac{u^2v^2-1}{8}\equiv\frac{u^2-1}{8}+\frac{v^2-1}{8}\qquad(\mathrm{mod}\ 2)$$

卽得.

定理 4. 若 m 與 n 爲二正奇數,且 $(m, n)=1$, 則

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{\frac{n-1}{2}\frac{m-1}{2}}.$$

證: 命 $m=\prod p$, $n=\prod q$, 則

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=\left(\prod_p\prod_q\left(\frac{p}{q}\right)\right)\left(\prod_p\prod_q\left(\frac{q}{p}\right)\right)=\prod_p\prod_q\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=$$

$$=\prod_p\prod_q(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}=(-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}$$

(此處用 (1) 式).

Legendre 符號之運用必須時時注意其分母是否是素數,而 Jacobi 符號則否,故如用 Jacobi 符號可以免分解因子之勞. 如:

$$\left(\frac{383}{443}\right)=-\left(\frac{443}{383}\right)=-\left(\frac{60}{383}\right)=-\left(\frac{2^2}{383}\right)\left(\frac{15}{383}\right)=-\left(\frac{15}{383}\right)=$$

$$=\left(\frac{383}{15}\right)=\left(\frac{8}{15}\right)=\left(\frac{2}{15}\right)=1.$$

如於定理 4 中取消 m, m' 爲正之條件,則有次之定理.

定理 5. 設 m, n 爲奇數, $(n, m)=1$. 若 m, n 皆爲負數,則

$$\left(\frac{n}{|m|}\right)\left(\frac{m}{|n|}\right)=-(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

不然其值爲

$$(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

讀者自證之.

例. 同餘式

$$x^2 \equiv -286 \qquad (\bmod 4272943)$$

有解否? 此處 4272943 爲素數,以 p 表之.

今欲求

$$\left(\frac{-286}{p}\right)$$

之值. 因 $\left(\frac{-1}{p}\right) = -1$, $\left(\frac{2}{p}\right) = 1$, 故

$$\left(\frac{-286}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{143}{p}\right) = -\left(\frac{143}{p}\right).$$

求 $\left(\frac{143}{p}\right)$ 之值可用下法:

$$4272943 = 29880 \times 143 + 103^*$$

$$143 = 2 \times 103 - 63$$

$$103 = 2 \times 63 - 23$$

$$63 = 2 \times 23 + 17^*$$

$$23 = 2 \times 17 - 11$$

$$17 = 2 \times 11 - 5^*$$

$$11 = 2 \times 5 + 1$$

(凡有星號 * 之步驟表示變號一次),故

$$\left(\frac{143}{p}\right) = (-1)^3 = -1.$$

即 $\left(\frac{-286}{p}\right) = 1$. 即該同餘式可解. Gauss 實際算出,其根爲 ± 1493445.

§ 7. 二項同餘式. 設 p 爲素數. 今往討論二項同餘式

$$x^k \equiv n \qquad (\bmod p).$$

定理 1. 同餘式

$$x^k \equiv 1 \qquad (\bmod p) \tag{1}$$

之根數等於 $(k, p-1)$.

證: 1) 命 $d=(k,p-1)$,必有二整數 s 及 t 使

$$sk+t(p-1)=d.$$

如此,則 $x^d=(x^k)^s\ (x^{p-1})^t$. 故凡 (1) 之根,必爲

$$x^d\equiv 1 \qquad (\bmod p) \tag{2}$$

之根. 反之,顯然.

2) 由 1) 可知如能證明 (2) 有 d 個根卽足. 由定理 2.9.1 已知 (2) 式之根數不超過 d. 又 $x^{p-1}\equiv 1\ (\bmod p)$ 之根數爲 $p-1$. 再由定理 2.9.1,

$$\frac{x^{p-1}-1}{x^d-1}=(x^d)^{\frac{p-1}{d}-1}+\cdots+x^d+1\equiv 0 \qquad (\bmod p)$$

之根數不超過 $p-1-d$, 故 (2) 式之根數 $\geqslant d$. 故得定理.

定理 2. 二項同餘式

$$x^k\equiv n \qquad (\bmod p), \qquad p\nmid n$$

或無解,或有 $(k,p-1)$ 個不同的解.

證: 若有一解 x_0, 則

$$(x_0^{-1}x)^k\equiv x^k x_0^{-k}\equiv 1 \qquad (\bmod p).$$

故由定理 1 得定理 2.

定理 3. 若 x 過模 p 之縮系,則 x^k 取 $(p-1)/(k,p-1)$ 個不同之值.

證: 由定理 2 已知有 $(k,p-1)$ 個不同餘之數,其 k 次方皆同餘, mod p. 故整個 $p-1$ 個不同餘之數分爲 $(p-1)/(k,p-1)$ 類. 每一類對應一數, mod p, 互不同餘.

定義. 設 h 爲一整數, $(n,h)=1$, 最小之正整數 l 使

$$h^l\equiv 1 \qquad (\bmod n)$$

者,名爲 h 對模 n 之次數,或 h 之次數, mod n.

定理 4. 若 $h^m\equiv 1\ (\bmod n)$, 則 $l|m$.

證: 不然必有二整數 q 及 r 使

$$m=ql+r \qquad 0<r<l,$$

而

$$h^r\equiv h^m(h^l)^{-q}\equiv 1 \qquad (\bmod n),$$

此與 l 之定義相違背.

定理 5. 設 $l|p-1$, 又設 $\varphi(l)$ 爲次數爲 l 的互不同餘之整數的個數,則此 $\varphi(l)$ 卽爲 Euler 函數.

證: 先證出 $\varphi(l)$ 之若干性質,再證明其爲 Euler 函數.

1) 若 $(l_1, l_2)=1$, 則 $\varphi(l_1l_2)=\varphi(l_1)\ \varphi(l_2)$. 命 h_1 及 h_2 之次數各爲 l_1 及 l_2. 設 h_1h_2 之次數爲 l. 由

$$1\equiv(h_1 h_2)^{ll_2}\equiv h_1^{ll_2} \pmod p,$$

由定理 4 可知 $l_1|ll_2$. 因 $(l_1,\ l_2)=1$, 故 $l_1|l$. 同法, $l_2|l$. 故 $l=l_1l_2$. 卽 h_1h_2 之次數爲 l_1l_2. 故如有一數 h_1 其次數是 l_1, 他一數 h_2 之次數是 l_2, 則可做出一數 h_1h_2 其次數爲 l_1l_2, 今證若非 $h_1\equiv h_1' \pmod p$, $h_2\equiv h_2' \pmod p$, 則

$$h_1 h_2\not\equiv h_1' h_2' \pmod p,$$

蓋若 $h_1 h_2\equiv h_1' h_2' \pmod p$, 則 $h_1 h_1'^{-1}\equiv h_2' h_2^{-1} \pmod p$. 但 $h_1 h_1'^{-1}$ 的次數$|l_1$, $h_2' h_2^{-1}$ 的次數$|l_2$, 故必

$$h_1 h_1'^{-1}\equiv h_2' h_2^{-1}\equiv 1 \pmod p,$$

而與假設相違背. 反之,若有一數 h, 其次數是 $l_1 l_2$, $(l_1, l_2)=1$. 則有 $h_1=h^{l_2}$, $h_2=h^{l_1}$, 其次數各爲 l_1, l_2. 故得 $\varphi(l_1)\ \varphi(l_2)=\varphi(l_1 l_2)$.

2) 設 $l=q^t$, q 爲素數,則

$$x^{q^t}-1\equiv 0 \pmod p$$

之根數爲 q^t, 若 x 適合此式而其次數非 q^t, 則必適合

$$x^{q^{t-1}}-1\equiv 0 \pmod p.$$

此式之根數爲 q^{t-1}. 故

$$\varphi(q^t)=q^t-q^{t-1}.$$

3) 合 1) 及 2) 二性質,可知 $\varphi(l)$ 卽爲 Euler 函數.

§ 8. 原根及指數.

由定理 7.5 知有 $\varphi(p-1)$ 個不同餘之數其次數是 $p-1$, mod p.

定義 1. 次數爲 $p-1$ 之數,謂之 p 之原根 (Primitive root).

命 g 爲 p 之一原根,則

$$g^0, g^1, \cdots, g^{p-2} \qquad (\text{mod } p)$$

必無兩個互相同餘.

定義 2. 任一整數 n $(p \nmid n)$, 必有一數 a 使

$$n \equiv g^a \qquad (\text{mod } p), \qquad 0 \leqslant a < p-1.$$

此 a 名爲 n 之指數, mod p. 以 $a = \text{ind}_g n$ 表之. (在不易引起混淆之處,常簡寫爲 ind n.) 若 b 爲任一數使

$$n \equiv g^b \qquad (\text{mod } p),$$

則

$$b \equiv \text{ind } n \qquad (\text{mod } p-1).$$

指數與通常之對數相彷,有次之性質:

1) $\text{ind } ab \equiv \text{ind } a + \text{ind } b$, $(\text{mod } p-1)$, $p \nmid ab$;

2) $\text{ind } a^l \equiv l \text{ ind } a$, $(\text{mod } p-1)$, $p \nmid a$.

(注意: 僅當 $p \nmid a$ 時, ind a 方有意義,此與不定義 log 0 同.)

定義 3. 命 $p \nmid n$. 若

$$x^k \equiv n \qquad (\text{mod } p), \qquad (1)$$

有解,則 n 謂之 p 之 k 次剩餘,不然則謂之 p 之 k 次非剩餘.

定理 1. n 爲 p 之 k 次剩餘之必要且充分之條件爲 $(k, p-1)$ 能整除 ind n.

證: 命 ind $x = y$, ind $n = a$, 則 (1) 與 $ky \equiv a$ $(\text{mod } p-1)$ 等價,而此式有解之充分且必要條件爲 $(k, p-1)$ 能整除 a. 故得定理.

"底數互換公式". 此處之指數顯然與所取之原根有關. 命 g_1 爲另一原根及 $g_1 \equiv g^b (\text{mod } p)$. 如此則

$$n \equiv g_1^a \equiv (g^b)^a \qquad (\text{mod } p),$$

卽

$$\text{ind}_g n \equiv ab \equiv \text{ind}_g g_1 \, \text{ind}_{g_1} n \qquad (\text{mod } p-1).$$

此與對數換底數之公式同.

玆將小於 5000 之素數之最小原根表附於本章末,以備參考.

§ 9. 縮系之構造. 設 m 爲一自然數. 問題:能否有一數 g 存在,使

$$g^0, g^1, g^2, \cdots, g^{\varphi(m)-1} \qquad (\bmod m)$$

表出模 m 之縮系? 若能存在,則如此之 g 名爲對模 m 之原根.

定 理 1. m 有原根存在之必要且充分之條件爲 $m=2, 4, p^l$ 及 $2p^l$ (此處 p 爲奇素數).

證: 1) 命 m 之標準分解式爲

$$m=p_1^{l_1} p_2^{l_2} \cdots p_s^{l_s}, \qquad p_1<p_2<\cdots<p_s.$$

由 Euler 定理, 任一整數 a, $(a, p_i)=1$, 必適合

$$a^{\varphi(p_i^{l_i})} \equiv 1 \qquad (\bmod p_i^{l_i}).$$

命 l 爲 $\varphi(p_1^{l_1}), \cdots, \varphi(p_s^{l_s})$ 之最小公倍數, 則

$$a^l \equiv 1 \qquad (\bmod m).$$

故若 $l<\varphi(m)$, 則無原根存在;若 $p>2$, 則 $\varphi(p^l)$ 爲偶數. 故 m 不能有兩個不同之奇素因子. 若 m 有原根, m 必爲 $2^l, p^l$ 或 $2^c p^l$ 之一. 若 $c \geqslant 2$, 則 $\varphi(2^c)=2^{c-1}$ 亦爲偶數, 而 $2^c p^l$ 亦不能有原根. 故僅有 $m=2^l$, p^l, $2p^l$ 三種可能性而已.

2) $m=2^l$. 若 $l=1$, 1 卽爲原根; 若 $l=2$, 3 卽爲原根; 若 $l \geqslant 3$, 則對諸奇數 a 有 $a^{2^{l-2}} \equiv 1 \ (\bmod 2^l)$. 今用歸納法證明此點: 若

$$a^{2^{l-3}}=1+2^{l-1}\lambda,$$

則

$$a^{2^{l-2}} \equiv (1+2^{l-1}\lambda)^2 \equiv 1 \qquad (\bmod 2^l).$$

故 $m=2^l$ $(l>2)$ 無原根.

3) 命 $m=p^l$. 由 §8 已知此定理對 $l=1$ 時爲眞. 命 g 爲 p 之原根: 若 $g^{p-1}-1 \not\equiv 0 \ (\bmod p^2)$, 卽取 $r=g$; 若 $g^{p-1}-1 \equiv 0 \ (\bmod p^2)$, 卽取 $r=g+p$. 如此則

$$r^{p-1}-1 \equiv (g+p)^{p-1}-1 \equiv -g^{p-2}p \not\equiv 0 \qquad (\bmod p^2).$$

故此 r 亦爲 p 之原根. 命

$$r^{p-1}-1=kp,\qquad p\nmid k.$$

因

$$(1+kp)^{p^s}\equiv 1+kp^{s+1}\pmod{p^{s+2}},\quad s\geqslant 0,$$

引用此理,可證明

$$(r^{p-1})^{p^s}\equiv 1+kp^{s+1}\pmod{p^{s+2}}.$$

即得

$$r^{p^{l-2}(p-1)}\equiv 1+kp^{l-1}\pmod{p^l},\quad l\geqslant 2.\tag{1}$$

若 r 之次數爲 e, 則 $e\,|\,(p-1)p^{l-1}=\varphi(p^l)$. 因 r 爲 p 之原根,故 $(p-1)\,|\,e$. 故由 (1) 可知 $e=\varphi(p^l)$,即 r 爲 p^l 之原根.

4) $m=2p^l$. 取 g 爲 p^l 之原根. 若 g 爲奇數, g 即爲 $2p^l$ 之原根; 若 g 爲偶數, $g+p^l$ 爲 $2p^l$ 之原根.

定理 2. 若 $l>2$, 則 5 對模 2^l 之次數爲 2^{l-2}.

證: 今先證: 當 $a\geqslant 3$,

$$5^{2^{a-3}}\equiv 1+2^{a-1}\pmod{2^a}.$$

當 $a=3$ 此爲顯然. 再用歸納法,

$$5^{2^{a-2}}=(5^{2^{a-3}})^2\equiv(1+2^{a-1}+k2^a)^2\equiv 1+2^a\pmod{2^{a+1}}.$$

故 $5^{2^{l-3}}\not\equiv 1\pmod{2^l}$ 而 $5^{2^{l-2}}\equiv 1\pmod{2^l}$. 即 5 之次數爲 2^{l-2}, mod 2^l.

定理 3. 設 $l>2$, 對任一奇數 a, 必有一 b 使

$$a\equiv(-1)^{\frac{a-1}{2}}5^b\pmod{2^l},\qquad b\geqslant 0.$$

證: 若 $a\equiv 1\pmod 4$, 由定理 2,

$$5^b,\qquad 0\leqslant b<2^{l-2}$$

給與 2^{l-2} 個不同數, mod 2^l. 且皆 $\equiv 1\pmod 4$. 故必有一 b 使 $a\equiv 5^b$ $\pmod{2^l}$.

若 $a\equiv 3\pmod 4$, 則 $-a\equiv 1\pmod 4$, 故由上述立得所求.

定理 4. 設 $m=2^l\cdot p_1^{l_1}\cdots p_s^{l_s}$ (標準分解式). $l\geqslant 0$, $l_1>0,\cdots,l_s>0$. 依 $l=0$, 1; $l=2$; 或 $l>2$ 以定義 $\delta=0,1$ 或 2. 則 m 之縮系,可由 $s+\delta$ 個數之乘方之積表出之.

證: 1) 設 $m=m'm''$, $(m',m'')=1$. 命

$$a_1, \cdots, a_{\varphi(m')}$$

爲 m' 之縮系,且 $a_i \equiv 1 \pmod{m''}$ (此常可能); 又命

$$b_1, \cdots, b_{\varphi(m'')}$$

爲 m'' 之縮系,且 $b_i \equiv 1 \pmod{m'}$,則

$$a_i b_j$$

卽表 $m' m''$ 之縮系. 其個數爲 $\varphi(m'm'')$. 又若

$$a_i b_j \equiv a_s b_t \pmod{m' m''},$$

則立得

$$a_i \equiv a_s \pmod{m'}, \qquad b_j \equiv b_t \pmod{m''}.$$

2) 由定理 1 及 3 可知: $m = p^l (p > 2)$ 之縮系可由一數之乘方得之; $m = 2^l$ (若 $l > 1$) 之縮系可由 δ 個數之乘方之積得之. 總此及 1),可知定理眞實.

此定理實質指出一重要原則,卽羣論中所謂之 Abel 羣之基礎定理也.

習題. 若 $k < p$, $n = k p^2 + 1$, 且

$$2^k \not\equiv 1, \quad 2^{n-1} \equiv 1 \pmod{n},$$

則 n 是一素數.

[提示: (i) 先證明 n 中有一素因子 $\equiv 1 \pmod{p}$. 命 d 爲最小之正整數使 $2^d \equiv 1 \pmod{n}$. 推得 $d \nmid k$, $d | n-1$ 及 $p | d$. 再由 $p | d | \varphi(n)$ 而得出結論; (ii) 由 $n = kp^2 + 1 = (up+1)(vp+1)$ 而證明 n 不可能是複合數.]

註: 取 $p = 2^{127} - 1$, $k = 180$. 有機械幫助 Miller 及 Wheeler 證明了 $180(2^{127}-1)^2 + 1$ 是素數. (*Nature* **168** (1951), 838 頁).

素數之最小原根表(5000之內者)

加*者表示 10 爲其原根

p	$p-1$	g	p	$p-1$	g	p	$p-1$	g
3	2	2	137	$2^3\cdot17$	3	311	$2\cdot5\cdot31$	17
5	2^2	2	139	$2\cdot3\cdot23$	2	313*	$2^3\cdot3\cdot13$	10
7*	$2\cdot3$	3	149*	$2^2\cdot37$	2	317	$2^2\cdot79$	2
11	$2\cdot5$	2	151	$2\cdot3\cdot5^2$	6	331	$2\cdot3\cdot5\cdot11$	3
13	$2^2\cdot3$	2	157	$2^2\cdot3\cdot13$	5	337*	$2^4\cdot3\cdot7$	10
17*	2^4	3	163	$2\cdot3^4$	2	347	$2\cdot173$	2
19*	$2\cdot3^2$	2	167*	$2\cdot83$	5	349	$2^2\cdot3\cdot29$	2
23*	$2\cdot11$	5	173	$2^2\cdot43$	2	353	$2^5\cdot11$	3
29*	$2^2\cdot7$	2	179*	$2\cdot89$	2	359	$2\cdot179$	7
31	$2\cdot3\cdot5$	3	181*	$2^2\cdot3^2\cdot5$	2	367*	$2\cdot3\cdot61$	6
37	$2^2\cdot3^2$	2	191	$2\cdot5\cdot19$	19	373	$2^2\cdot3\cdot31$	2
41	$2^3\cdot5$	6	193*	$2^6\cdot3$	5	379*	$2\cdot3^3\cdot7$	2
43	$2\cdot3\cdot7$	3	197	$2^2\cdot7^2$	2	383*	$2\cdot191$	5
47*	$2\cdot23$	5	199	$2\cdot3^2\cdot11$	3	389*	$2^2\cdot97$	2
53	$2^2\cdot13$	2	211	$2\cdot3\cdot5\cdot7$	2	397	$2^2\cdot3^2\cdot11$	5
59*	$2\cdot29$	2	223*	$2\cdot3\cdot37$	3	401	$2^4\cdot5^2$	3
61*	$2^2\cdot3\cdot5$	2	227	$2\cdot113$	2	409	$2^3\cdot3\cdot17$	21
67	$2\cdot3\cdot11$	2	229*	$2^2\cdot3\cdot19$	6	419*	$2\cdot11\cdot19$	2
71	$2\cdot5\cdot7$	7	233*	$2^3\cdot29$	3	421	$2^2\cdot3\cdot5\cdot7$	2
73	$2^3\cdot3^2$	5	239	$2\cdot7\cdot17$	7	431	$2\cdot5\cdot43$	7
79	$2\cdot3\cdot13$	3	241	$2^4\cdot3\cdot5$	7	433*	$2^4\cdot3^3$	5
83	$2\cdot41$	2	251	$2\cdot5^3$	6	439	$2\cdot3\cdot73$	15
89	$2^3\cdot11$	3	257*	2^8	3	443	$2\cdot13\cdot17$	2
97*	$2^5\cdot3$	5	263*	$2\cdot131$	5	449	$2^6\cdot7$	3
101	$2^2\cdot5^2$	2	269*	$2^2\cdot67$	2	457	$2^3\cdot3\cdot19$	13
103	$2\cdot3\cdot17$	5	271	$2\cdot3^3\cdot5$	6	461*	$2^2\cdot5\cdot23$	2
107	$2\cdot53$	2	277	$2^2\cdot3\cdot23$	5	463	$2\cdot3\cdot7\cdot11$	3
109*	$2^2\cdot3^3$	6	281	$2^3\cdot5\cdot7$	3	467	$2\cdot233$	2
113*	$2^4\cdot7$	3	283	$2\cdot3\cdot47$	3	479	$2\cdot239$	13
127	$2\cdot3^2\cdot7$	3	293	$2^2\cdot73$	2	487*	$2\cdot3^5$	3
131*	$2\cdot5\cdot13$	2	307	$2\cdot3^2\cdot17$	5	491*	$2\cdot5\cdot7^2$	2

p	$p-1$	g	p	$p-1$	g	p	$p-1$	g
499*	$2\cdot3\cdot83$	7	719	$2\cdot359$	11	947	$2\cdot11\cdot43$	2
503*	$2\cdot251$	5	727*	$2\cdot3\cdot11^2$	5	953*	$2^3\cdot7\cdot17$	3
509*	$2^2\cdot127$	2	733	$2^2\cdot3\cdot61$	6	967	$2\cdot3\cdot7\cdot23$	5
521	$2^3\cdot5\cdot13$	3	739	$2\cdot3^2\cdot41$	3	971*	$2\cdot5\cdot97$	6
523	$2\cdot3^2\cdot29$	2	743*	$2\cdot7\cdot53$	5	977*	$2^4\cdot61$	3
541*	$2^2\cdot3^3\cdot5$	2	751	$2\cdot3\cdot5^3$	3	983*	$2\cdot491$	5
547	$2\cdot3\cdot7\cdot13$	2	757	$2^2\cdot3^3\cdot7$	2	991	$2\cdot3^2\cdot5\cdot11$	6
557	$2^2\cdot139$	2	761	$2^3\cdot5\cdot19$	6	997	$2^2\cdot3\cdot83$	7
563	$2\cdot281$	2	769	$2^8\cdot3$	11	1009	$2^4\cdot3^2\cdot7$	11
569	$2^3\cdot71$	3	773	$2^2\cdot193$	2	1013	$2^2\cdot11\cdot23$	3
571*	$2\cdot3\cdot5\cdot19$	3	787	$2\cdot3\cdot131$	2	1019*	$2\cdot509$	2
577*	$2^6\cdot3^2$	5	797	$2^2\cdot199$	2	1021*	$2^2\cdot3\cdot5\cdot17$	10
587	$2\cdot293$	2	809	$2^3\cdot101$	3	1031	$2\cdot5\cdot103$	14
593*	$2^4\cdot37$	3	811*	$2\cdot3^4\cdot5$	3	1033*	$2^3\cdot3\cdot43$	5
599	$2\cdot13\cdot23$	7	821*	$2^2\cdot5\cdot41$	2	1039	$2\cdot3\cdot173$	3
601	$2^3\cdot3\cdot5^2$	7	823*	$2\cdot3\cdot137$	3	1049	$2^3\cdot131$	3
607	$2\cdot3\cdot101$	3	827	$2\cdot7\cdot59$	2	1051*	$2\cdot3\cdot5^2\cdot7$	7
613	$2^2\cdot3^2\cdot17$	2	829	$2^2\cdot3^2\cdot23$	2	1061	$2^2\cdot5\cdot53$	2
617	$2^3\cdot7\cdot11$	3	839	$2\cdot419$	11	1063*	$2\cdot3^2\cdot59$	3
619*	$2\cdot3\cdot103$	2	853	$2^2\cdot3\cdot71$	2	1069*	$2^2\cdot3\cdot89$	6
631	$2\cdot3^2\cdot5\cdot7$	3	857*	$2^3\cdot107$	3	1087*	$2\cdot3\cdot181$	3
641	$2^7\cdot5$	3	859	$2\cdot3\cdot11\cdot13$	2	1091*	$2\cdot5\cdot109$	2
643	$2\cdot3\cdot107$	11	863*	$2\cdot431$	5	1093	$2^2\cdot3\cdot7\cdot13$	5
647*	$2\cdot17\cdot19$	5	877	$2^2\cdot3\cdot73$	2	1097*	$2^3\cdot137$	3
653	$2^2\cdot163$	2	881	$2^4\cdot5\cdot11$	3	1103*	$2\cdot19\cdot29$	5
659*	$2\cdot7\cdot47$	2	883	$2\cdot3^2\cdot7^2$	2	1109*	$2^2\cdot277$	2
661	$2^2\cdot3\cdot5\cdot11$	2	887*	$2\cdot443$	5	1117	$2^2\cdot3^2\cdot31$	2
673	$2^5\cdot3\cdot7$	5	907	$2\cdot3\cdot151$	2	1123	$2\cdot3\cdot11\cdot17$	2
677	$2^2\cdot13^2$	2	911	$2\cdot5\cdot7\cdot13$	17	1129	$2^3\cdot3\cdot47$	11
683	$2\cdot11\cdot31$	5	919	$2\cdot3^3\cdot17$	7	1151	$2\cdot5^2\cdot23$	17
691	$2\cdot3\cdot5\cdot23$	3	929	$2^5\cdot29$	3	1153*	$2^7\cdot3^2$	5
701*	$2^2\cdot5^2\cdot7$	2	937*	$2^3\cdot3^2\cdot13$	5	1163	$2\cdot7\cdot83$	5
709*	$2^2\cdot3\cdot59$	2	941*	$2^2\cdot5\cdot47$	2	1171*	$2\cdot3^2\cdot5\cdot13$	2

p	$p-1$	g	p	$p-1$	g	p	$p-1$	g
1181*	$2^2\cdot5\cdot59$	7	1433*	$2^3\cdot179$	3	1657	$2^3\cdot3^2\cdot23$	11
1187	$2\cdot593$	2	1439	$2\cdot719$	7	1663*	$2\cdot3\cdot277$	3
1193*	$2^3\cdot149$	3	1447*	$2\cdot3\cdot241$	3	1667	$2\cdot7^2\cdot17$	2
1201	$2^4\cdot3\cdot5^2$	11	1451	$2\cdot5^2\cdot29$	2	1669	$2^2\cdot3\cdot139$	2
1213*	$2^2\cdot3\cdot101$	2	1453	$2^2\cdot3\cdot11^2$	2	1693	$2^2\cdot3^2\cdot47$	2
1217*	$2^6\cdot19$	3	1459	$2\cdot3^6$	5	1697*	$2^5\cdot53$	3
1223*	$2\cdot13\cdot47$	5	1471	$2\cdot3\cdot5\cdot7^2$	6	1699	$2\cdot3\cdot283$	3
1229*	$2^2\cdot307$	2	1481	$2^3\cdot5\cdot37$	3	1709*	$2^2\cdot7\cdot61$	3
1231	$2\cdot3\cdot5\cdot41$	3	1483	$2\cdot3\cdot13\cdot19$	2	1721	$2^3\cdot5\cdot43$	3
1237	$2^2\cdot3\cdot103$	2	1487*	$2\cdot743$	5	1723	$2\cdot3\cdot7\cdot41$	3
1249	$2^5\cdot3\cdot13$	7	1489	$2^4\cdot3\cdot31$	14	1733	$2^2\cdot433$	2
1259*	$2\cdot17\cdot37$	2	1493	$2^2\cdot373$	2	1741*	$2^2\cdot3\cdot5\cdot29$	2
1277	$2^2\cdot11\cdot29$	2	1499	$2\cdot7\cdot107$	2	1747	$2\cdot3^2\cdot97$	2
1279	$2\cdot3^2\cdot71$	3	1511	$2\cdot5\cdot151$	11	1753	$2^3\cdot3\cdot73$	7
1283	$2\cdot641$	2	1523	$2\cdot761$	2	1759	$2\cdot3\cdot293$	6
1289	$2^3\cdot7\cdot23$	6	1531*	$2\cdot3^2\cdot5\cdot17$	2	1777*	$2^4\cdot3\cdot37$	5
1291*	$2\cdot3\cdot5\cdot43$	2	1543*	$2\cdot3\cdot257$	5	1783*	$2\cdot3^4\cdot11$	10
1297*	$2^4\cdot3^4$	10	1549*	$2^2\cdot3^2\cdot43$	2	1787	$2\cdot19\cdot47$	2
1301*	$2^2\cdot5^2\cdot13$	2	1553*	$2^4\cdot97$	3	1789*	$2^2\cdot3\cdot149$	6
1303*	$2\cdot3\cdot7\cdot31$	6	1559	$2\cdot19\cdot41$	19	1801	$2^3\cdot3^2\cdot5^2$	11
1307	$2\cdot653$	2	1567*	$2\cdot3^3\cdot29$	3	1811*	$2\cdot5\cdot181$	6
1319	$2\cdot659$	13	1571*	$2\cdot5\cdot157$	2	1823*	$2\cdot911$	5
1321	$2^3\cdot3\cdot5\cdot11$	13	1579*	$2\cdot3\cdot263$	3	1831	$2\cdot3\cdot5\cdot61$	3
1327*	$2\cdot3\cdot13\cdot17$	3	1583*	$2\cdot7\cdot113$	5	1847*	$2\cdot13\cdot71$	5
1361	$2^4\cdot5\cdot17$	3	1597	$2^2\cdot3\cdot7\cdot19$	11	1861*	$2^2\cdot3\cdot5\cdot31$	2
1367*	$2\cdot683$	5	1601	$2^6\cdot5^2$	3	1867	$2\cdot3\cdot311$	2
1373	$2^2\cdot7^3$	2	1607*	$2\cdot11\cdot73$	5	1871	$2\cdot5\cdot11\cdot17$	14
1381*	$2^2\cdot3\cdot5\cdot23$	2	1609	$2^3\cdot3\cdot67$	7	1873*	$2^4\cdot3^2\cdot13$	10
1399	$2\cdot3\cdot233$	13	1613	$2^2\cdot13\cdot31$	3	1877	$2^2\cdot7\cdot67$	2
1409	$2^7\cdot11$	3	1619*	$2\cdot809$	2	1879	$2\cdot3\cdot313$	6
1423	$2\cdot3^2\cdot79$	3	1621*	$2^2\cdot3^4\cdot5$	2	1889	$2^5\cdot59$	3
1427	$2\cdot23\cdot31$	2	1627	$2\cdot3\cdot271$	3	1901	$2^2\cdot3^2\cdot19$	2
1429*	$2^2\cdot3\cdot7\cdot17$	6	1637	$2^2\cdot409$	2	1907	$2\cdot953$	2

p	$p-1$	g	p	$p-1$	g	p	$p-1$	g
1913*	$2^3\cdot239$	3	2161	$2^4\cdot3^3\cdot5$	23	2417*	$2^4\cdot151$	3
1931	$2\cdot5\cdot193$	2	2179*	$2\cdot3^2\cdot11^2$	7	2423*	$2\cdot7\cdot173$	5
1933	$2^2\cdot3\cdot7\cdot23$	5	2203	$2\cdot3\cdot367$	5	2437*	$2^2\cdot3\cdot7\cdot29$	2
1949*	$2^2\cdot487$	2	2207*	$2\cdot1103$	5	2441	$2^3\cdot5\cdot61$	6
1951	$2\cdot3\cdot5^2\cdot13$	3	2213	$2^2\cdot7\cdot79$	2	2447*	$2\cdot1223$	5
1973	$2^2\cdot17\cdot29$	2	2221*	$2^2\cdot3\cdot5\cdot37$	2	2459*	$2\cdot1229$	2
1979*	$2\cdot23\cdot43$	2	2237	$2^2\cdot13\cdot43$	2	2467	$2\cdot3^2\cdot137$	2
1987	$2\cdot3\cdot331$	2	2239	$2\cdot3\cdot373$	3	2473*	$2^3\cdot3\cdot103$	5
1993*	$2^3\cdot3\cdot83$	5	2243	$2\cdot19\cdot59$	2	2477	$2^2\cdot619$	2
1997	$2^2\cdot499$	2	2251*	$2\cdot3^2\cdot5^3$	7	2503	$2\cdot3^2\cdot139$	3
1999	$2\cdot3^3\cdot37$	3	2267	$2\cdot11\cdot103$	2	2521	$2^3\cdot3^2\cdot5\cdot7$	17
2003	$2\cdot7\cdot11\cdot13$	5	2269*	$2^2\cdot3^4\cdot7$	2	2531	$2\cdot5\cdot11\cdot23$	2
2011	$2\cdot3\cdot5\cdot67$	3	2273*	$2^5\cdot71$	3	2539*	$2\cdot3^3\cdot47$	2
2017*	$2^5\cdot3^2\cdot7$	5	2281	$2^3\cdot3\cdot5\cdot19$	7	2543*	$2\cdot31\cdot41$	5
2027	$2\cdot1013$	2	2287	$2\cdot3^2\cdot127$	19	2549*	$4\cdot7^2\cdot13$	2
2029*	$2^2\cdot3\cdot13^2$	2	2293	$2^2\cdot3\cdot191$	2	2551	$2\cdot3\cdot5^2\cdot17$	6
2039	$2\cdot1019$	7	2297*	$2^3\cdot7\cdot41$	5	2557	$2^2\cdot3^2\cdot71$	2
2053	$2^2\cdot3^3\cdot19$	2	2309*	$2^2\cdot577$	2	2579*	$2\cdot1289$	2
2063*	$2\cdot1031$	5	2311	$2\cdot3\cdot5\cdot7\cdot11$	3	2591	$2\cdot5\cdot7\cdot37$	7
2069*	$2^2\cdot11\cdot47$	2	2333	$2^2\cdot11\cdot53$	2	2593*	$2^5\cdot3^4$	7
2081	$2^5\cdot5\cdot13$	3	2339*	$2\cdot7\cdot167$	2	2609	$2^4\cdot163$	3
2083	$2\cdot3\cdot347$	2	2341*	$2^2\cdot3^2\cdot5\cdot13$	7	2617*	$2^3\cdot3\cdot109$	5
2087	$2\cdot7\cdot149$	5	2347	$2\cdot3\cdot17\cdot23$	3	2621*	$2^2\cdot5\cdot131$	2
2089	$2^3\cdot3^2\cdot29$	7	2351	$2\cdot5^2\cdot47$	13	2633*	$2^3\cdot7\cdot47$	3
2099*	$2\cdot1049$	2	2357	$2^2\cdot19\cdot31$	2	2647	$2\cdot3^3\cdot7^2$	3
2111	$2\cdot5\cdot211$	7	2371*	$2\cdot3\cdot5\cdot79$	2	2657*	$2^5\cdot83$	3
2113*	$2^6\cdot3\cdot11$	5	2377	$2^3\cdot3^3\cdot11$	5	2659	$2\cdot3\cdot443$	2
2129	$2^4\cdot7\cdot19$	3	2381	$2^2\cdot5\cdot7\cdot17$	3	2663*	$2\cdot11^3$	5
2131	$2\cdot3\cdot5\cdot71$	2	2383*	$2\cdot3\cdot397$	5	2671	$2\cdot3\cdot5\cdot89$	7
2137*	$2^3\cdot3\cdot89$	10	2389*	$2^2\cdot3\cdot199$	2	2677	$2^2\cdot3\cdot223$	2
2141*	$2^2\cdot5\cdot107$	2	2393	$2^3\cdot13\cdot23$	3	2683	$2\cdot3^2\cdot149$	2
2143*	$2\cdot3^2\cdot7\cdot17$	3	2399	$2\cdot11\cdot109$	11	2687*	$2\cdot17\cdot79$	5
2153*	$2^3\cdot269$	3	2411*	$2\cdot5\cdot241$	6	2689	$2^7\cdot3\cdot7$	19

p	$p-1$	g	p	$p-1$	g	p	$p-1$	g
2693	$2^2\cdot673$	2	2953	$2^3\cdot3^2\cdot41$	13	3251*	$2\cdot5^3\cdot13$	6
2699*	$2\cdot19\cdot71$	2	2957	$2^2\cdot739$	2	3253	$2^2\cdot3\cdot271$	2
2707	$2\cdot3\cdot11\cdot41$	2	2963	$2\cdot1481$	2	3257*	$2^3\cdot11\cdot37$	3
2711	$2\cdot5\cdot271$	7	2969	$2^3\cdot7\cdot53$	3	3259*	$2\cdot3\ 181$	3
2713*	$2^3\cdot3\cdot113$	5	2971*	$2\cdot3^3\cdot5\cdot11$	10	3271	$2\cdot3\cdot5\cdot109$	3
2719	$2\cdot3^2\cdot151$	3	2999	$2\cdot1499$	17	3299*	$2\cdot17\cdot97$	2
2729*	$2^3\cdot11\cdot31$	3	3001	$2^3\cdot3\cdot5^3$	14	3301*	$2^2\cdot3\cdot5^2\cdot11$	6
2731	$2\cdot3\cdot5\cdot7\cdot13$	3	3011*	$2\cdot5\cdot7\cdot43$	2	3307	$2\cdot3\cdot19\cdot29$	2
2741*	$2^2\cdot5\cdot137$	2	3019*	$2\cdot3\cdot503$	2	3313*	$2^4\cdot3^2\cdot23$	10
2749	$2^2\cdot3\cdot229$	6	3023*	$2\cdot1511$	5	3319	$2\cdot3\cdot7\cdot79$	6
2753*	$2^6\cdot43$	3	3037	$2^2\cdot3\cdot11\cdot23$	2	3323	$2\cdot11\cdot151$	2
2767*	$2\cdot3\cdot461$	3	3041	$2^5\cdot5\cdot19$	3	3329	$2^8\cdot13$	3
2777*	$2^3\cdot347$	3	3049	$2^3\cdot3\cdot127$	11	3331*	$2\cdot3^2\cdot5\cdot37$	3
2789*	$2^2\cdot17\cdot41$	2	3061	$2^2\cdot3^2\cdot5\cdot17$	6	3343*	$2\cdot3\cdot557$	5
2791	$2\cdot3^2\cdot5\cdot31$	6	3067	$2\cdot3\cdot7\cdot73$	2	3347	$2\cdot7\cdot239$	2
2797	$2^2\cdot3\cdot233$	2	3079	$2\cdot3^4\cdot19$	6	3359	$2\cdot23\cdot73$	11
2801	$2^4\cdot5^2\cdot7$	3	3083	$2\cdot23\cdot67$	2	3361	$2^5\cdot3\cdot5\cdot7$	22
2803	$2\cdot3\cdot467$	2	3089	$2^4\cdot193$	3	3371*	$2\cdot5\cdot337$	2
2819*	$2\cdot1409$	2	3109	$2^2\cdot3\cdot7\cdot37$	6	3373	$2^2\cdot3\cdot281$	5
2833*	$2^4\cdot3\cdot59$	5	3119	$2\cdot1559$	7	3389*	$2^2\cdot7\cdot11^2$	3
2837	$2^2\cdot709$	2	3121	$2^4\cdot3\cdot5\cdot13$	7	3391	$2\cdot3\cdot5\cdot113$	3
2843	$2\cdot7^2\cdot29$	2	3137*	$2^6\cdot7^2$	3	3407*	$2\cdot13\cdot131$	5
2851*	$2\cdot3\cdot5^2\cdot19$	2	3163	$2\cdot3\cdot17\cdot31$	3	3413	$2^2\cdot853$	2
2857	$2^3\cdot3\cdot7\cdot17$	11	3167*	$2\cdot1583$	5	3433*	$2^3\cdot3\cdot11\cdot13$	5
2861*	$2^2\cdot5\cdot11\cdot13$	2	3169	$2^2\cdot3^2\cdot11$	7	3449	$2^3\cdot431$	3
2879	$2\cdot1439$	7	3181	$2^2\cdot3\cdot5\cdot53$	7	3457	$2^7\cdot3^3$	7
2887	$2\cdot3\cdot13\cdot37$	5	3187	$2\cdot3^3\cdot59$	2	3461*	$2^2\cdot5\cdot173$	2
2897*	$2^4\cdot181$	3	3191	$2\cdot5\cdot11\cdot29$	11	3463*	$2\cdot3\cdot577$	3
2903*	$2\cdot1451$	5	3203	$2\cdot1601$	2	3467	$2\cdot1733$	2
2909*	$2^2\cdot727$	2	3209	$2^3\cdot401$	3	3469*	$2^2\cdot3\cdot17^2$	2
2917	$2^2\cdot3^6$	5	3217	$2^4\cdot3\cdot67$	5	3491	$2\cdot5\cdot349$	2
2927*	$2\cdot7\cdot11\cdot19$	5	3221*	$2^2\cdot5\cdot7\cdot23$	10	3499	$2\cdot3\cdot11\cdot53$	2
2939*	$2\cdot13\cdot113$	2	3229	$2^2\cdot3\cdot269$	6	3511	$2\cdot3^3\cdot5\cdot13$	7

p	$p-1$	g	p	$p-1$	g	p	$p-1$	g
3517	$2^2\cdot3\cdot293$	2	3767	$2\cdot7\cdot269$	5	4027	$2\cdot3\cdot11\cdot61$	3
3527*	$2\cdot41\cdot43$	5	3769	$2^3\cdot3\cdot157$	7	4049	$2^4\cdot11\cdot23$	3
3529	$2^3\cdot3^2\cdot7^2$	17	3779*	$2\cdot1889$	2	4051*	$2\cdot3^4\cdot5^2$	10
3533	$2^2\cdot883$	2	3793	$2^4\cdot3\cdot79$	5	4057*	$2^3\cdot3\cdot13^2$	5
3539*	$2\cdot29\cdot61$	2	3797	$2^2\cdot13\cdot73$	2	4073*	$2^3\cdot509$	3
3541	$2^2\cdot3\cdot5\cdot59$	7	3803	$2\cdot1901$	2	4079	$2\cdot2039$	11
3547	$2\cdot3^2\cdot197$	2	3821*	$2^2\cdot5\cdot191$	3	4091*	$2\cdot5\cdot409$	2
3557	$2^2\cdot7\cdot127$	2	3823	$2\cdot3\cdot7^2\cdot13$	3	4093	$2^2\cdot3\cdot11\cdot31$	2
3559	$2\cdot3\cdot593$	3	3833*	$2^3\cdot479$	3	4099	$2\cdot3\cdot683$	2
3571*	$2\cdot3\cdot5\cdot7\cdot17$	2	3847*	$2\cdot3\cdot641$	5	4111	$2\cdot3\cdot5\cdot137$	17
3581*	$2^2\cdot5\cdot179$	2	3851*	$2\cdot5^2\cdot7\cdot11$	2	4127	$2\cdot2063$	5
3583	$2\cdot3^2\cdot199$	3	3853	$2^2\cdot3^2\cdot107$	2	4129	$2^5\cdot3\cdot43$	13
3593*	$2^3\cdot449$	3	3863*	$2\cdot1931$	5	4133	$2^2\cdot1033$	2
3607*	$2\cdot3\cdot601$	5	3877	$2^2\cdot3\cdot17\cdot19$	2	4139*	$2\cdot2069$	2
3613	$2^2\cdot3\cdot7\cdot43$	2	3881	$2^3\cdot5\cdot97$	13	4153*	$2^3\cdot3\cdot173$	5
3617*	$2^5\cdot113$	3	3889	$2^4\cdot3^5$	11	4157	$2^2\cdot1039$	2
3623*	$2\cdot1811$	5	3907	$2\cdot3^2\cdot7\cdot31$	2	4159	$2\cdot3^3\cdot7\cdot11$	3
3631	$2\cdot3\cdot5\cdot11^2$	21	3911	$2\cdot5\cdot17\cdot23$	13	4177*	$2^4\cdot3^2\cdot29$	5
3637	$2^2\cdot3^2\cdot101$	2	3917	$2^2\cdot11\cdot89$	2	4201	$2^3\cdot3\cdot5^2\cdot7$	11
3643	$2\cdot3\cdot607$	2	3919	$2\cdot3\cdot653$	3	4211*	$2\cdot5\cdot421$	6
3659*	$2\cdot31\cdot59$	2	3923	$2\cdot37\cdot53$	2	4217*	$2^3\cdot17\cdot31$	3
3671	$2\cdot5\cdot367$	13	3929	$2^3\cdot491$	3	4219*	$2\cdot3\cdot19\cdot37$	2
3673*	$2^3\cdot3^3\cdot17$	5	3931	$2\cdot3\cdot5\cdot131$	2	4229*	$2^2\cdot7\cdot151$	2
3677	$2^2\cdot919$	2	3943*	$2\cdot3^3\cdot73$	3	4231	$2\cdot3^2\cdot5\cdot47$	3
3691	$2\cdot3^2\cdot5\cdot41$	2	3947	$2\cdot1973$	2	4241	$2^4\cdot5\cdot53$	3
3697	$2^4\cdot3\cdot7\cdot11$	5	3967*	$2\cdot3\cdot661$	6	4243	$2\cdot3\cdot7\cdot101$	2
3701*	$2^2\cdot5^2\cdot37$	2	3989*	$2^2\cdot997$	2	4253	$2^2\cdot1063$	2
3709*	$2^2\cdot3^2\cdot103$	2	4001	$2^5\cdot5^3$	3	4259*	$2\cdot2129$	2
3719	$2\cdot11\cdot13^2$	7	4003	$2\cdot3\cdot23\cdot29$	2	4261*	$2^2\cdot3\cdot5\cdot71$	2
3727*	$2\cdot3^4\cdot23$	3	4007*	$2\cdot2003$	5	4271	$2\cdot5\cdot7\cdot61$	7
3733	$2^2\cdot3\cdot311$	2	4013	$2^2\cdot17\cdot59$	2	4273	$2^4\cdot3\cdot89$	5
3739	$2\cdot3\cdot7\cdot89$	7	4019*	$2\cdot7^2\cdot41$	2	4283	$2\cdot2141$	2
3761	$2^4\cdot5\cdot47$	3	4021	$2^2\cdot3\cdot5\cdot67$	2	4289	$2^6\cdot67$	3

p	$p-1$	g	p	$p-1$	g	p	$p-1$	g
4297	$2^3\cdot3\cdot179$	5	4549	$2^2\cdot3\cdot379$	6	4789	$2^2\cdot3^2\cdot7\cdot19$	2
4327*	$2\cdot3\cdot7\cdot103$	3	4561	$2^4\cdot3\cdot5\cdot19$	11	4793*	$2^3\cdot599$	3
4337*	$2^4\cdot271$	3	4567*	$2\cdot3\cdot761$	3	4799	$2\cdot2399$	7
4339*	$2\cdot3^2\cdot241$	10	4583*	$2\cdot29\cdot79$	5	4801	$2^6\cdot3\cdot5^2$	7
4349*	$2^2\cdot1087$	2	4591	$2\cdot3^3\cdot5\cdot17$	11	4813	$2^2\cdot3\cdot401$	2
4357	$2^2\cdot3^2\cdot11^2$	2	4597	$2^2\cdot3\cdot383$	5	4817*	$2^4\cdot7\cdot43$	3
4363	$2\cdot3\cdot727$	2	4603	$2\cdot3\cdot13\cdot59$	2	4831	$2\cdot3\cdot5\cdot7\cdot23$	3
4373	$2^2\cdot1093$	2	4621	$2^2\cdot3\cdot5\cdot7\cdot11$	2	4861	$2^2\cdot3^5\cdot5$	11
4391	$2\cdot5\cdot439$	14	4637	$2^2\cdot19\cdot61$	2	4871	$2\cdot5\cdot487$	11
4397	$2^2\cdot7\cdot157$	2	4639	$2\cdot3\cdot773$	3	4877	$2^2\cdot23\cdot53$	2
4409	$2^3\cdot19\cdot29$	3	4643	$2\cdot11\cdot211$	5	4889	$2^3\cdot13\cdot47$	3
4421*	$2^2\cdot5\cdot13\cdot17$	3	4649	$2^3\cdot7\cdot83$	3	4903	$2\cdot3\cdot19\cdot43$	3
4423*	$2\cdot3\cdot11\cdot67$	3	4651*	$2\cdot3\cdot5^2\cdot31$	3	4909	$2^2\cdot3\cdot409$	6
4441	$2^3\cdot3\cdot5\cdot37$	21	4657	$2^4\cdot3\cdot97$	15	4919	$2\cdot2459$	13
4447*	$2\cdot3^2\cdot13\cdot19$	3	4663	$2\cdot3^2\cdot7\cdot37$	3	4931*	$2\cdot5\cdot17\cdot29$	6
4451*	$2\cdot5^2\cdot89$	2	4673*	$2^6\cdot73$	3	4933	$2^2\cdot3^2\cdot137$	2
4457*	$2^3\cdot557$	3	4679	$2\cdot2339$	11	4937*	$2^3\cdot617$	3
4463*	$2\cdot23\cdot97$	5	4691*	$2\cdot5\cdot7\cdot67$	2	4943*	$2\cdot7\cdot358$	7
4481	$2^7\cdot5\cdot7$	3	4703*	$2\cdot2351$	5	4951	$2\cdot3^2\cdot5^2\cdot11$	6
4483	$2\cdot3^3\cdot83$	2	4721	$2^4\cdot5\cdot59$	6	4957	$2^2\cdot3\cdot7\cdot59$	2
4493	$2^2\cdot1123$	2	4723	$2\cdot3\cdot787$	2	4967*	$2\cdot13\cdot191$	5
4507	$2\cdot3\cdot751$	2	4729	$2^3\cdot3\cdot197$	17	4969	$2^3\cdot3^3\cdot23$	11
4513	$2^5\cdot3\cdot47$	7	4733	$2^2\cdot7\cdot13^2$	5	4973	$2^2\cdot11\cdot113$	2
4517	$2^2\cdot1129$	2	4751	$2\cdot5^3\cdot19$	19	4987	$2\cdot3^2\cdot277$	2
4519	$2\cdot3^2\cdot251$	3	4759	$2\cdot3\cdot13\cdot61$	3	4993	$2^7\cdot3\cdot13$	5
4523	$2\cdot7\cdot17\cdot19$	5	4783*	$2\cdot3\cdot797$	6	4999	$2\cdot3\cdot7^2\cdot17$	3
4547	$2\cdot2273$	2	4787	$2\cdot2393$	2			

第 四 章

多 項 式 之 性 質

§1. 多項式之整除性. 今往討論以有理數爲係數的多項式. 以 $\partial^\circ f$ 表多項式 $f(x)$ 之次數.

定義 1. 命 $f(x)$ 及 $g(x)$ 爲二多項式, $g(x)$ 不恆爲零. 若有一多項式 $h(x)$ 使

$$f(x) = g(x)\,h(x),$$

則謂 $g(x)$ 可整除 $f(x)$. 以

$$g(x)\mid f(x) \quad 或 \quad g\mid f$$

表之. 以 $g\nmid f$ 表 g 不能整除 f. 顯然有

(i) $f|f$;

(ii) 若 $f|g$ 及 $g|f$, 則 f 與 g 僅相差一常數因子, 如此之二多項式謂之相結合的多項式;

(iii) 若 $f|g$, $g|h$ 則 $f|h$;

(iv) 若 $f|g$, 則

$$\partial^\circ f \leqslant \partial^\circ g.$$

若 $f|g$ 而 $g\nmid f$, 則 f 名爲 g 之眞因子,顯然有 $\partial^\circ f < \partial^\circ g$.

定理 1. 任與二多項式 $f(x)$ 與 $g(x)$, $g(x)$ 不恆爲零,必有二多項式 $q(x)$ 及 $r(x)$ 使

$$f = q\cdot g + r,$$

此處 $r=0$ 或 $\partial^\circ r < \partial^\circ g$.

證: 可以依照 f 之次數行歸納法. 若 $\partial^\circ f < \partial^\circ g$, 則取 $q=0$, $r=f$, 自毋待證明.

若 $\partial^\circ f \geqslant \partial^\circ g$, 命

$$f = \alpha_n x^n + \cdots, \qquad \partial^\circ f = n,$$

$$g=\beta_m x^m+\cdots,\quad \partial^\circ g=m,$$

則

$$\partial^\circ(f-\alpha_n\beta_m^{-1}x^{n-m}g)<\partial^\circ f,$$

由歸納法之假定,有二多項式 $h(x)$ 及 $r(x)$ 存在使

$$f-\alpha_n\beta_m^{-1}x^{n-m}g=hg+r,$$

此處 $r=0$ 或 $\partial^\circ r<\partial^\circ g$. 如此則

$$f=(h+\alpha_n\beta_m^{-1}x^{n-m})g+r.$$

$$(q(x)=h(x)+\alpha_n\beta_m^{-1}x^{n-m}.)$$

明所欲證.

定義 2. 一多項式的集合 I, 如適合以下之條件,名爲一理想集合 (ideal):

(i) 若 f, g 爲 I 中之多項式,則 $f+g$ 亦在其中;

(ii) 若 f 爲 I 中之多項式, h 爲任一多項式,則 fh 亦在其中.

例. 一多項式 $f(x)$ 之諸倍式,成一理想集合.

定理 2. 任一理想集合中可以覓出一多項式 f, 使凡此集合中之多項式必爲 f 之倍式,卽該集合是 f 的諸倍式所組成的.

證: 命 f 爲此理想集合中之次數最低者. 若 g 爲此集合中之任一多項式而非 f 之倍式,則由定理 1 可知有二多項式 $q(x)$ 及 $r(x)$ $(\neq 0)$ 使

$$g=q\cdot f+r,\qquad \partial^\circ r<\partial^\circ f.$$

因 f 在此理想集合中,由 (ii) 可知 qf 亦在其中,更由 (i) $g-qf$ 亦在其中,卽 r 在此理想集合之中. 但 r 之次數低於 f 之次數,此與假定相違背. 故得定理.

定義 3. 命 f 及 g 爲二多項式. 取形如 $mf+ng$ 之多項式所成的集合(此處 m 及 n 皆爲多項式). 由以上之定理可知此爲一多項式 d 之倍式所成之集合. 此式名爲 f 及 g 之最大公約式,以 $(f,g)=d$ 表之. 爲使其唯一決定起見,取 (f,g) 之最高方之係數爲 1.

定理 3. (f,g) 有次之性質:

(i) 有二多項式 m 及 n 使 $(f, g) = mf + ng$;

(ii) 對任二多項式 m 及 n 必有 $(f, g) | mf + ng$;

(iii) 若 $l|f$, $l|g$ 則 $l|(f, g)$.

證: (i) 及 (ii) 可由定理 2 得之, (iii) 可由 (i) 得之.

定義 4. 若 $(f, g) = 1$, 則 f 與 g 名爲互素.

定理 4. 若 p 爲一不可化多項式,且 $p|fg$, 則 $p|f$ 或 $p|g$.

證: 若 $p \nmid f$, 則 $(f, p) = 1$. 故由定理 3 (i), 有二多項式 m 及 n 使

$$mf + np = 1,$$

故

$$mfg + ngp = g,$$

因 $p|fg$, 可知 $p|g$. 故得定理.

§2. 唯一分解定理.

定理 1. 任一多項式皆可分解爲不可化多項式之積. 若互相結合的多項式算作相同,並不計因子之次序,則此種分解法是唯一的.

證: 1) 分解性. 於 f 之次數上行歸納法. 若 f 不可分解,則毋待證明. 若 f 可分解,命

$$f = gh, \quad \partial^\circ g < \partial^\circ f; \quad \partial^\circ h < \partial^\circ f.$$

由歸納法之假定,已知 g 及 h 皆可分解爲不可化多項式之積.

2) 唯一性. 仍於 f 之次數上行歸納法. 假定

$$f = c_1 p_1^{a_1} \cdots p_k^{a_k} = c_2 q_1^{b_1} \cdots q_l^{b_l},$$

此式中 p 及 q 皆爲不可化多項式, 其最高方之係數爲 1, 且 p_i 與 p_j $(i \neq j)$ 不同, q_i 與 q_j $(i \neq j)$ 不同. 由定理 1.4, p_1 必與 $q_1, \cdots, q_l$ 中之一相結合, 假定其卽爲 q_1, 由於其最高方之係數爲 1, 故 $p_1 = q_1$. 卽得

$$\frac{f}{p_1} = c_1 p_1^{a_1-1} p_2^{a_2} \cdots p_k^{a_k} = c_2 q_1^{b_1-1} \cdots q_l^{b_l}$$

因爲 $\frac{f}{p_1}$ 之次數低於 f. 故由歸納法得出定理.

定理 2. 設 $f(x)$ 與 $g(x)$ 爲二個有有理係數的多項式, 且 $f(x)$ 爲不可化,若 $f(x) = 0$ 與 $g(x) = 0$ 有公共根,則必

$$f(x) \mid g(x).$$

證：因 $f(x)=0$ 與 $g(x)=0$ 有公共根，故 $(f(x),\ g(x))\neq 1$. 命 $d(x)$ 爲 $f(x), g(x)$ 的最大公因式，則因 $f(x)$ 爲不可化，故必 $d(x)$ 與 $f(x)$ 相結合。所以

$$f(x)\mid g(x).$$

由此定理立刻可得：若 $f(x)$ 爲一 n 次不可化多項式．而以

$$\vartheta^{(1)},\ \vartheta^{(2)},\cdots,\vartheta^{(n)}$$

表示 $f(x)=0$ 所有的根，則必 $\vartheta^{(i)}\neq\vartheta^{(j)}$ $(i\neq j)$. 且若某一 $\vartheta^{(i)}$ 適合另一有理係數方程式 $g(x)=0$, 則 $f(x)=0$ 的其他 $n-1$ 個根亦必適合此方程式．

定理 3. 命 f 及 g 皆爲最高方之係數是 1 的多項式：

$$f=p_1^{a_1}\cdots p_s^{a_s},\qquad a_\nu\geqslant 0,$$

$$g=p_1^{b_1}\cdots p_s^{b_s},\qquad b_\nu\geqslant 0,$$

式中 p_ν 是不相等的不可化多項式，且其最高方之係數等於 1，則

$$(f,g)=p_1^{c_1}\cdots p_s^{c_s},$$

此處 $c_\nu=\min(a_\nu, b_\nu)$.

此定理之證明極易，從略．

定義 1. 命 f, g 爲二多項式．f 及 g 皆能整除之多項式名爲此二式之公倍式．其中次數最低者稱爲最小公倍式，以 $[f,g]$ 表其中最高方之係數爲 1 者．

定理 4. 一如定理 3 之假定，可得

$$[f,g]=p_1^{d_1}\cdots p_s^{d_s};$$

此處 $d_\nu=\max(a_\nu, b_\nu)$.

由此立得：

定理 5. 二多項式之任一公倍式．必爲此二多項式之最小公倍式所整除．

定理 6. 若 f, g 爲二多項式，其最高方之係數爲 1，則

$$fg=[f,g]\,(f,g).$$

習題 1. 由第一章之內容試擬若干習題．

習題 2. 試將理想集合的觀念推廣到含多個變數的多項式．並舉例證明定理 1.2 並不眞實．

提示：二多項式

$$f(x, y, z) = 0, \quad g(x, y, z) = 0$$

之軌跡代表一空間代數曲線. 形如 $mf + ng$ 之多項式所成之理想集合 I, 有次之性質: 此代數曲線上之點使 I 中任一多項式等於 0.

§ 3. 同餘式.

命 $m(x)$ 爲一多項式. 若

$$m(x) \mid f(x) - g(x),$$

則謂 $f(x)$ 與 $g(x)$ 對模 $m(x)$ 同餘,以

$$f(x) \equiv g(x) \quad (\mathrm{mod}\ m(x))$$

表之. 對任一模 $m(x)$ 顯然有

(i) f 與其自己同餘;

(ii) 若 f 與 g 同餘,則 g 與 f 也同餘;

(iii) 若 f 與 g 同餘, g 與 h 同餘, 則 f 與 h 也同餘;

(iv) 若

$$f \equiv g, \quad f_1 \equiv g_1 \quad (\mathrm{mod}\ m),$$

則

$$f \pm f_1 \equiv g \pm g_1 \quad (\mathrm{mod}\ m),$$

$$f f_1 \equiv g g_1 \quad (\mathrm{mod}\ m).$$

此諸結果之證明從略 (參考 §2.2).

對模 $m(x)$, 可分多項式爲剩餘類: 每一類中之多項式皆對模 $m(x)$ 同餘, 屬於不同類中之一多項式必不同餘. (iv) 建議諸類之間可定義加減及乘. 顯然,此諸類所成之集合對加減乘而言自封. 以 0 表 $m(x)$ 所能整除的多項式所成的剩餘類.

若 $m(x)$ 不可化,更可證明: 剩餘類所成之集合中也可定義除法 (當然,除數非 0). 切實言之,若 $f(x)$ 非 $m(x)$ 之倍數,則有二多項式 $a(x)$ 及 $b(x)$ 使

$$a(x) f(x) + b(x) m(x) = 1.$$

卽有多項式 $a(x)$ 使

$$a(x) f(x) \equiv 1 \quad (\mathrm{mod}\ m(x)).$$

故得

定理 1. 若 $m(x)$ 爲不可化,凡非 0 之剩餘類,必有其唯一的逆類. 切實

言之，命 A 表一非 0 之剩餘類，必有一類 B 存在，使 A, B 中各取一多項式 $f(x)$ 及 $g(x)$ 常有次之關係:

$$f(x)\,g(x)\equiv 1 \qquad (\mathrm{mod}\, m(x)).$$

今更舉例以明本節之內容: 取 $m(x)=x^2+1$. 此乃一不可化多項式. 任一剩餘類中必有一唯一的多項式:

$$ax+b.$$

換言之, $ax+b$ 可以表所有的剩餘類. 類間的和差之定義如次:

$$ax+b\pm(a_1x+b_1)=(a\pm a_1)\,x+(b\pm b_1).$$

其積

$$(ax+b)\,(a_1x+b_1)=aa_1x^2+(ab_1+a_1b)\,x+bb_1$$
$$\equiv(ab_1+a_1b)\,x+bb_1-aa_1 \qquad (\mathrm{mod}\, x^2+1).$$

因此，如以有理數對 (a, b) 表一剩餘類之包有 $ax+b$ 者，則其間加減乘之關係如次:

$$(a,b)\pm(a_1,b_1)=(a\pm a_1,\, b\pm b_1),$$
$$(a,b)\,(a_1,b_1)=(ab_1+ba_1,\, bb_1-aa_1).$$

由於

$$(ax+b)\,(-ax+b)\equiv a^2+b^2 \qquad (\mathrm{mod}\, x^2+1),$$

所以 (a, b) 之逆類是 $\left(-\frac{a}{a^2+b^2}, \frac{b}{a^2+b^2}\right)$. 換言之，與複數 $ai+b$ 之四則運算全同.

根據此處所建立之原則，若 $m(x)$ 爲一 n 次多項式，其最高方的係數爲 1, 則任一剩餘類必包有一個多項式其次數小於 n, 並且僅有一個. 故所謂模 $m(x)$ 之諸剩餘類之討論可以看成爲形如

$$\alpha_1 x^{n-1}+\alpha_2 x^{n-2}+\cdots+\alpha_{n-1}x+\alpha_n$$

之多項式之討論. 二如此元素之和卽爲由其對應係數求和所得出之多項式，其積卽爲由普通之求積法所得出之多項式以 $m(x)$ 除之所得出之最低次餘式.

習題 1. 設 $\alpha_1, \alpha_2, \alpha_3$ 各不相同. 求一二次多項式 $f(x)$ 適合於

$$f(\alpha_1)=\beta_1, \qquad f(\alpha_2)=\beta_2, \qquad f(\alpha_3)=\beta_3.$$

並說明其與大衍求一術之關係.

解答：

$$f(x)=\beta_1\frac{(x-\alpha_2)(x-\alpha_3)}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)}+\beta_2\frac{(x-\alpha_3)(x-\alpha_1)}{(\alpha_2-\alpha_3)(\alpha_2-\alpha_1)}+\beta_3\frac{(x-\alpha_1)(x-\alpha_2)}{(\alpha_3-\alpha_1)(\alpha_3-\alpha_2)}.$$

此乃 Lagrange 插入公式.

習題 2. 設 $m_1(x)$ 與 $m_2(x)$ 爲二不互相結合之不可化多項式. 命 $f_1(x)$ 及 $f_2(x)$ 爲所與之多項式. 證明必有一多項式 $f(x)$ 使

$$f(x)\equiv f_1(x)\qquad(\bmod m_1(x)),$$
$$f(x)\equiv f_2(x)\qquad(\bmod m_2(x)).$$

習題 3. 試推廣以上二習題.

§4. 整係數多項式.

顯然所有的整係數多項式對加減乘自封.

一組整係數多項式適合以下條件時,謂之成一理想集合:

(i) 若 f, g 在此集合之中,則 $f+g$ 亦然;

(ii) 若 f 在此集合中,而 g 爲任一整係數多項式,則 fg 亦在此集合中.

定理 1 (Hilbert). 在一理想集合 A 中必有有限個整係數多項式 $f_1,\cdots,f_n$ 具有次之性質: A 中任一多項式 f 必可表爲

$$f=g_1f_1+g_2f_2+\cdots+g_nf_n,$$

此處 $g_1,\cdots,g_n$ 也是整係數多項式.

證: 1) 在 A 中諸多項式之最高方之係數成爲一集合 B, 此集合爲整數所成的模,何則? 若 a, b 在此集合中,其對應的多項式爲

$$f(x)=a\,x^n+\cdots,\qquad g(x)=b\,x^m+\cdots.$$

則由 (ii) 可知 $f(x)x^m$, $g(x)x^n$ 皆在 A 中,即

$$f(x)\,x^m\pm g(x)\,x^n=(a\pm b)\,x^{m+n}+\cdots$$

也在 A 中, 而此式之最高方之係數爲 $a\pm b$. 因此證明 B 是一模. 由定理 1.4.3, 可知 B 中有一正整數 d, 使凡 B 中之數皆爲 d 之倍數. 命以此 d 爲最高方之係數的多項式爲

$$f_1=dx^l+d_1x^{l-1}+\cdots+d_{l-1}x+d_l.$$

2) 對 A 中之任一多項式 f, 必有二整係數之多項式 $q(x)$ 及 $r(x)$, 使

$$f(x)=q(x)\,f_1(x)+r(x),$$

此處 $\partial^\circ r<\partial^\circ f_1$ 或 $r=0$. 何則? 若 $f(x)$ 之次數低於 $f_1(x)$ 之次數, 自毋待言. 若

$$f(x)=ax^n+a_1x^{n-1}+\cdots+a_n,\qquad n\geqslant l,$$

則由 1) 已知 $d|a$, 而

$$f(x)-\frac{a}{d}x^{n-l}f_1(x)$$

爲一多項式, 其次數 $\leqslant n-1$. 若其次數仍大於 l, 則其最高方之係數仍爲 d 之倍數. 故可續行此法以得 2) 之結論.

3) 若 A 中無低於 l 次之多項式,則定理已明. 不然,命 d' 爲 A 中所有低於 l 次之多項式之最高方之係數的最大公約數,又命

$$f_2=d'x^{l'}+\alpha_1'x^{l'-1}+\cdots\qquad(d\mid d')$$

爲其對應之多項式. 用上法可知,凡 A 中次數小於 l 而不小於 l' 之多項式 f 必可表爲

$$f(x)=q(x)\,f_2(x)+r(x),$$

此處 $q(x)$, $r(x)$ 皆是整係數多項式,且 $\partial^\circ r<\partial^\circ f_2$ 或 $r=0$.

續行此法可得定理.

習題 1. 試將定理 1 推廣到 n 個變數之情況.

習題 2. 試將定理 1 中之整係數多項式換爲整值多項式而研究其正確性.

§ 5. 以素數爲模之多項式.

本節所論之多項式皆有整係數. 且設 p 是一固定素數.

定義 1. 若二多項式 $f(x)$ 及 $g(x)$ 之對應係數皆對模 p 同餘,則此二式謂之對模 p 同餘,以

$$f(x)\equiv g(x)\pmod p$$

表之. 例如

$$7x^2+16x+9\equiv 2x+2\pmod 7.$$

$f(x)$ 之最高方之係數非 p 之倍數者, 名爲此多項式對模 p 的次數, 以 $\partial^\circ f$ 表之. 例如,對模 7,

$$\partial^\circ(7x^2+16x+9)=1,$$

但對模 3,

$$\partial^\circ(7x^2+16x+9)=2.$$

如此所定義的同餘關係顯然有次之諸性質:

(i) $f(x)\equiv f(x) \pmod p$;

(ii) 若 $f\equiv g \pmod p$, 則 $g\equiv f \pmod p$;

(iii) 若 $f\equiv g$, $g\equiv h \pmod p$, 則 $f\equiv h \pmod p$;

(iv) 若 $f\equiv g$, $f_1\equiv g_1 \pmod p$, 則

$$f\pm f_1\equiv g\pm g_1 \pmod p$$

及

$$f f_1\equiv g g_1 \pmod p.$$

特别值得注意者爲

$$(f(x))^p\equiv f(x^p) \pmod p.$$

定義 2. 命 $f(x)$ 及 $g(x)$ 爲二多項式, $g(x)$ 不恆爲零, mod p. 若有一多項式 $h(x)$ 使

$$f(x)\equiv h(x)\,g(x) \pmod p,$$

則謂 $g(x)$ 可整除 $f(x)$, mod p. 而稱 $g(x)$ 爲 $f(x)$ 之因式, mod p, 以 $g(x)\mid f(x)$, mod p. 表之.

例如: 由於

$$x^5+3x^4-4x^3+2\equiv(2x^2-3)(3x^3-x^2+1) \pmod 5,$$

可知

$$2x^2-3\mid x^5+3x^4-4x^3+2 \pmod 5.$$

顯然有

(i) $f(x)\mid f(x)$ mod p;

(ii) 若 $f(x)\mid g(x)$ mod p, 及 $g(x)\mid f(x)$ mod p, 則 $f(x)$ 與 $g(x)$ 僅相差一常數因子. 卽有一整數 a 使

$$f(x)\equiv ag(x) \pmod p.$$

如是之二式名爲互相結合, mod p. 顯然任一多項式共有 $p-1$ 個多項式與之相結合, mod p, 而其中有一個 (且唯有一個) 其最高方的係數爲 1;

(iii) 若 $f\mid g$ mod p, $g\mid h$ mod p, 則 $f\mid h$ mod p;

(iv) 任與二多項式 $f(x)$, $g(x)$, $g(x)$ 不恆爲零, mod p, 必有二多項式 $q(x)$ 與 $r(x)$ 使

$$f(x) \equiv q(x)\, g(x) + r(x) \qquad (\mathrm{mod}\ p),$$

此處 $r(x) \equiv 0 \pmod p$ 或 $\partial^\circ r < \partial^\circ g$.

定義 3. 若一 n 次多項式 $f(x)$ 不能分解爲兩個低於 n 次多項式之積, mod p, 則此多項式稱爲對模 p 不可化多項式,或對模 p 素多項式.

例如: 若取 $p = 3$, 則不互相結合的一次式有 3:

$$x, \qquad x+1, \qquad x+2,$$

皆不可化. 不互相結合的二次式有 9:

$$\begin{array}{lll} x^2, & x^2+x, & x^2+2x, \\ x^2+1, & x^2+x+1, & x^2+2x+1, \\ x^2+2, & x^2+x+2, & x^2+2x+2. \end{array}$$

其中可化者有 $6(=(x+a)(x+b))$,而不可化者有 3:

$$x^2+1, \qquad x^2+x+2, \qquad x^2+2x+2.$$

注意: 一多項式對模 p 不可化,則原來也必不可化,由此證出, x^2+2x+2 無有理根.

已與一 p, 求出有多少個 n 次不可化多項式, mod p, 乃一極有趣味的問題, 將於 §9 中解決之.

定理 1. 任一多項式可以分解爲不可化多項式之積, mod p. 舍結合關係及次序外,此分解法是唯一的.

證明與定理 2.1 的證明同,故從略.

與 §1 同法,可定義最大公約式及最小公倍式. 以 (f, g) 表 f, g 之最大公約式之最高方係數爲 1 者,並可證明

定理 2. 有二多項式 $m(x)$ 及 $n(x)$ 使

$$m(x)\, f(x) + n(x)\, g(x) \equiv (f(x), g(x)) \qquad (\mathrm{mod}\ p).$$

§6. 若干關於分解之定理.

定義 1. 命

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots$$

表一多項式. 多項式

$$na_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots$$

稱爲 $f(x)$ 的導數,以 $f'(x)$ 表之.

顯然有

$$(f(x) + g(x))' = f'(x) + g'(x). \tag{1}$$

由於

$$\begin{aligned}(x^m \cdot x^n)' &= (m+n)\, x^{n+m-1} \\ &= (m\, x^{m-1})\, x^n + (n\, x^{n-1})\, x^m \\ &= (x^m)'\, x^n + (x^n)'\, x^m, \end{aligned} \tag{2}$$

可以證明

$$(f(x)\, g(x))' = f'(x)\, g(x) + g'(x)\, f(x). \tag{3}$$

蓋如命

$$f(x) = \sum_{i=0}^{n} a_i x^i, \qquad g(x) = \sum_{j=0}^{m} b_j x^j,$$

則由 (1) 可知

$$(f(x)\, g(x))' = \sum_{i=0}^{n} a_i (x^i\, g(x))' = \sum_{i=0}^{n} a_i \sum_{j=0}^{m} b_j (x^{i+j})'.$$

再由 (2) 及 (1) 可知

$$\begin{aligned}(f(x)\, g(x))' &= \sum_{i=0}^{n} a_i \sum_{j=0}^{m} b_j ((x^i)'\, x^j + (x^j)'\, x^i) \\ &= \sum_{i=0}^{n} a_i (x^i)' \sum_{j=0}^{m} b_j x^j + \sum_{i=0}^{n} a_i x^i \Big(\sum_{j=0}^{m} b_j x^j\Big)' \\ &= f'(x)\, g(x) + g'(x)\, f(x). \end{aligned}$$

定義 2. 若一多項式 $f(x)$ 能爲另一非常數之多項式之平方所整除, mod p, 則 $f(x)$ 名爲有重因子, mod p.

例如: $x^5 + x^4 - x^3 - x^2 + x + 1$ 對模 3 有重因子 $(x^2+1)^2$.

定理 1. $f(x)$ 有重因子之必要且充分條件爲 $(f(x), f'(x))$ 之次數 $\geqslant 1$.

證: 1) 假定 $f(x)$ 有重因子,即

$$f(x) \equiv P^2(x) Q(x) \pmod p,$$

其導數爲

$$f'(x) \equiv 2P(x)P'(x)Q(x) + P^2(x)Q'(x) \pmod p,$$

故 $f(x)$，$f'(x)$ 有公因子 $P(x) \bmod p$.

2) 假定 $P(x)$ 爲 $(f(x),\ f'(x))$ 之不可化因子，mod p, 且

$$f(x) \equiv P(x)\ Q(x) \pmod p, \quad P(x) \nmid Q(x) \pmod p,$$

則

$$f'(x) \equiv P'(x)\ Q(x) + Q'(x)\ P(x) \pmod p.$$

由 $P(x) \mid f'(x) \bmod p$, 可知 $P(x) \mid P'(x) Q(x) \bmod p$. 由於 $P(x) \nmid Q(x) \bmod p$, 可知

$$P(x) \mid P'(x) \pmod p.$$

由於 $P'(x)$ 之次數低於 $P(x)$ 之次數，故必 $P'(x) \equiv 0 \pmod p$，故 $P(x)$ 的形式一定是

$$P(x) = \sum_{l=0}^{m} a_l x^{pl}.$$

由於

$$P(x) \equiv \left(\sum_{l=0}^{m} a_l x^l \right)^p \pmod p,$$

可知 $P(x)$ 並非不可化，這與假定相違背．定理已經證明．

定理 2. 若 $p \nmid n$, 則 $x^n - 1$ 無重因子，mod p.

證：命 n' 是適合

$$n n' \equiv 1 \pmod p$$

之整數，則

$$\begin{aligned}(x^n - 1,\ nx^{n-1}) &= (x^n - 1 - n'nx^{n-1}x,\ nx^{n-1}) \\ &= (-1,\ nx^{n-1}) = 1.\end{aligned}$$

由定理 1 推出本定理.

定理 3 命 $(m, n) = d$, 則

$$(x^m - 1,\ x^n - 1) = x^d - 1.$$

證：若 $m = n$, 此定理顯然眞實.

命 $N = \max(m, n)$. 今於 N 上施用歸納法．假定 $n > m$. 由歸納法假定可知

$$\begin{aligned}(x^m - 1,\ x^n - 1) &= (x^m - 1,\ x^n - 1 - x^{n-m}(x^m - 1)) \\ &= (x^m - 1,\ x^{n-m} - 1)\end{aligned}$$

$$= (x^{d'} - 1),$$

此處

$$d' = (m, n - m) = (m, n) = d.$$

定理 4. 命 $(m, n) = d$, 則

$$(x^{p^m-1} - 1, x^{p^n-1} - 1) = x^{p^d-1} - 1.$$

證: 命 $l = (p^m - 1, p^n - 1)$. 由定理 3 可知

$$(x^{p^m-1} - 1, x^{p^n-1} - 1) = x^l - 1.$$

再如定理 3 之證法,可知

$$l = (p^m - 1, p^n - 1) = p^d - 1.$$

§ 7. 重模同餘式.

定義 1. 命 p 表一素數, $\varphi(x)$ 爲一多項式. 若 $f_1(x) - f_2(x)$ 爲 $\varphi(x)$ 之倍式, mod p, 則謂之 f_1 及 f_2 對重模 $p, \varphi(x)$ 同餘,記之如:

$$f_1(x) \equiv f_2(x) \qquad (\text{modd}\, p, \varphi(x)).$$

例如:

$$x^5 + 3x^4 + x^2 + 4x + 3 \equiv 0 \qquad (\text{modd}\, 5, 2x^2 - 3).$$

顯然有次之諸性質:

1) $f(x) \equiv f(x) \qquad (\text{modd}\, p, \varphi(x))$;

2) 若 f 與 g 對重模 $p, \varphi(x)$ 同餘,則 g 與 f 亦然;

3) 若 f 與 g 及 g 與 h 皆對重模 $p, \varphi(x)$ 同餘,則 f 與 h 亦然;

4) 若

$$f(x) \equiv g(x), \quad f_1(x) \equiv g_1(x) \qquad (\text{modd}\, p, \varphi(x)),$$

則

$$f(x) \pm f_1(x) \equiv g(x) \pm g_1(x) \qquad (\text{modd}\, p, \varphi(x)),$$

及

$$f(x)\, f_1(x) \equiv g(x)\, g_1(x) \qquad (\text{modd}\, p, \varphi(x));$$

5) 設 $\varphi(x)$ 對 p 之次數爲 n. 任一多項式必與下列多項式之一

$$a_1 + a_2 x + \cdots + a_n x^{n-1}, \qquad 0 \leqslant a_i \leqslant p - 1 \tag{1}$$

同餘. 顯然 (1) 表 p^n 個多項式,其中無二者對重模 $p, \varphi(x)$ 同餘,且任一多項式必與其中之一同餘, modd $p, \varphi(x)$.

定義 2. 由 (1) 所表出的 p^n 個多項式稱爲重模 $p, \varphi(x)$ 之完全剩餘系. 一完全剩餘系中除去與 $\varphi(x)$ 非互素者稱爲重模 $p, \varphi(x)$ 之縮系.

定理 1. 若 $f(x)$ 過重模 $p, \varphi(x)$ 之完全剩餘系, 且 $(g(x), \varphi(x))=1$, 則 $g(x)f(x)$ 也過一完全剩餘系. 若 $f(x)$ 過縮系, 則 $g(x)f(x)$ 也過一縮系.

證: 若

$$g(x) f_1(x) \equiv g(x) f_2(x) \qquad (\text{modd}\, p, \varphi(x)),$$

則由於 $\varphi(x) \nmid g(x) \bmod p$, 可知

$$f_1(x) \equiv f_2(x) \qquad (\text{modd}\, p, \varphi(x)).$$

由此性質易於獲得本定理之證明.

習題. 試推廣 Euler 函數之定義. 進而求出其表示公式.

§ 8. Fermat 定理之推廣.

設 p 爲一素數, $\varphi(x)$ 爲 n 次不可化多項式, mod p.

定理 1. 對任一非 $\varphi(x)$ 之倍式之多項式 $f(x)$, mod p, 恆有

$$(f(x))^{p^n-1} \equiv 1 \qquad (\text{modd}\, p, \varphi(x)).$$

對任一多項式常有

$$(f(x))^{p^n} \equiv f(x) \qquad (\text{modd}\, p, \varphi(x)). \tag{1}$$

特別有

$$x^{p^n} \equiv x \qquad (\text{modd}\, p, \varphi(x)). \tag{2}$$

證: 命

$$f_1(x), \cdots, f_{p^n-1}(x), \qquad (\text{modd}\, p, \varphi(x))$$

爲一縮系, modd p, $\varphi(x)$. 則

$$f f_1, \cdots, f f_{p^n-1}$$

亦爲一縮系. 故

$$\prod_{i=1}^{p^n-1} f_i(x) \equiv \prod_{i=1}^{p^n-1} (f(x) f_i(x)) \qquad (\text{modd}\, p, \varphi(x)),$$

即

$$((f(x))^{p^n-1}-1) \prod_{i=1}^{p^n-1} f_i(x) \equiv 0 \qquad (\text{modd}\, p, \varphi(x)).$$

故

$$(f(x))^{p^n-1} \equiv 1 \qquad (\text{modd}\, p, \varphi(x)).$$

此乃第一章 Fermat 定理之推廣.

注意: (2) 固然是 (1) 之特例,但 (2) 也可直接推出 (1) 來: 蓋

$$(f(x))^{p^n} \equiv f(x^{p^n}) \equiv f(x) \qquad (\text{modd } p, \varphi(x))$$

故也.

習題. 試推廣第二章中之 Euler 定理.

定理 2. 任一 n 次不可化多項式一定整除 $x^{p^n-1}-1$, mod p. 此定理可由定理 1 直接推出.

定理 3. 重模方程

$$f(X) \equiv 0 \qquad (\text{modd } p, \varphi(x))$$

之根之個數不超過 $f(X)$ 之次數.

證: 若 $g(x)$ 是此式之一根,命

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots,$$

則

$$f(X) = f(X) - f(g(x)) = a_n(X^n - (g(x))^n) + a_{n-1}(X^{n-1} - (g(x))^{n-1}) + \cdots$$
$$= (X - g(x))\, h(X)\,.$$

若 $g_1(x)$ 是另一根 $\neq g(x)$, 則得

$$h(g_1(x)) \equiv 0 \qquad (\text{modd } p, \varphi(x)),$$

由此可證出本定理.

定理 4. $x^{p^n-1}-1$ 不爲一高於 n 次之不可化多項式所整除, mod p.

證: 設 $\psi(x)$ 是一不可化多項式, mod p, 其次數 $m > n$, 且假定

$$x^{p^n} \equiv x \qquad (\text{modd } p, \psi(x))\,.$$

對重模 p, $\psi(x)$ 有 p^m 個互不同餘之多項式 $f(x)$. 因 $(f(x))^p \equiv f(x^p)$ mod p, 故

$$(f(x))^{p^n} \equiv f(x^{p^n}) \equiv f(x) \qquad (\text{modd } p, \psi(x))\,.$$

卽 $X^{p^n} \equiv X$ (modd p, $\psi(x)$) 之根數爲 p^m 而大於 p^n, 此不可能.

定理 5. 若 $\psi(x)$ 爲一 l 次不可化多項式, mod p, 且

$$\psi(x) \mid x^{p^n} - x \qquad (\text{mod } p),$$

則 $l \mid n$.

證：由定理 2 及本定理之假定

$$\psi(x) \mid (x^{p^n-1}-1,\ x^{p^l-1}-1) \qquad (\bmod p),$$

由定理 6.3

$$\psi(x) \mid x^{p^d-1}-1 \quad (\bmod p), \quad d=(n, l).$$

更由定理 4，可知 $l \leqslant d=(n, l)$. 故 $l=d$，卽 $l|n$.

習題. 設 $\psi(x)$ 及 $\varphi(x)$ 都是不可化多項式，mod p，則

$$\psi(X) \equiv 0 \qquad (\text{modd } p, \varphi(x))$$

可解之必要且充分之條件爲 $\partial^\circ\psi|\partial^\circ\varphi$. 並證若可解則可分解爲一次因子之積.

§9. 對模 p 之不可化多項式.

定理 1. 所有的 n 次不可化多項式，mod p，之積等於

$$\frac{x^{p^n}-x}{\prod\limits_{q_1}(x^{p^{n/q_1}}-x)} \frac{\prod\limits_{q_1,q_2}(x^{p^{n/q_1q_2}}-x)}{\prod\limits_{q_1,q_2,q_3}(x^{p^{n/q_1q_2q_3}}-x)} \cdots \qquad (\bmod p),$$

此處 $q_1, q_2, \cdots$ 過 n 之不同的素因子.

證：由定理 6.1，$x^{p^n}-x$ 無重因子，故可分解爲若干個不同的不可化多項式

$$\psi(x)=x^d+a_1x^{d-1}+\cdots$$

之積. 而 $\psi(x)|x^{p^d}-x$, $d|n$.

今用 §1.7 之逐步淘汰原則：已知 $x^{p^n}-x$ 爲諸 m $(m|n)$ 次不可化多項式之積. 於其中除去所有的多項式之次數整除 $\frac{n}{q_1}$ 者，但以 $\frac{n}{q_1q_2}$ 之因子爲次數之多項式已除了兩次，故又必需添上，等等.

定理 2. 共有

$$\frac{1}{n}\left(p^n-\sum_{q_1}p^{n/q_1}+\sum_{q_1,q_2}p^{n/q_1q_2}-\sum p^{n/q_1q_2q_3}+\cdots\right)$$

個 n 次不可化多項式，此處 $\sum\limits_{q_1}$ 過 n 之所有的素因子，$\sum\limits_{q_1,q_2}$ 過 n 的所有的不等的素因子對 $q_1\,q_2$，等等.

證：定理 1 中之多項式之次數是

$$N=p^n-\sum_{q_1}p^{n/q_1}+\cdots, \tag{1}$$

其每一因子之次數爲 n，故得定理.

命

$$n = q_1^{l_1} \cdots q_s^{l_s},$$

此處 q_i 爲 n 的各不相等之素因子. 顯然

$$N \equiv (-1)^s p^{n/q_1 \cdots q_s} \pmod{p^{n/q_1 \cdots q_s + 1}}.$$

故 $N > 0$. 是以

定理 3. 必有一 n 次不可分解多項式存在.

習題. 無遺漏地補出下一節中所略去的證明.

§ 10. 原根.

本節中所述與第三章 §8 所論者頗多相似，故將詳細證明留諸讀者.

設 $(f(x), \varphi(x)) = 1$，若有一多項式 $g(x)$ 存在，使

$$(g(x))^m \equiv f(x) \quad (\text{modd } p, \varphi(x)),$$

則 $f(x)$ 名爲 m 次剩餘，modd p，$\varphi(x)$.

$f(x)$ 是二次剩餘之必要且充分之條件是

$$(f(x))^{\frac{1}{2}(p^n-1)} \equiv 1 \quad (\text{modd } p, \varphi(x)),$$

不然

$$(f(x))^{\frac{1}{2}(p^n-1)} \equiv -1 \quad (\text{modd } p, \varphi(x)).$$

定義. 最小之正整數 l 使

$$(f(x))^l \equiv 1 \quad (\text{modd } p, \varphi(x))$$

者名爲 $f(x)$ 所屬的次數.

如前可證 l 乃 $p^n - 1$ 之因子，並可證明屬於次數 l 的多項式之個數等於 $\varphi(l)$. 因此有 $\varphi(p^n - 1)$ 個多項式屬於次數 $p^n - 1$. 這種的多項式名爲原根 (modd p. $\varphi(x)$). 若 $f(x)$ 是一原根，則

$$(f(x))^\nu, \quad \nu = 1, 2, \cdots, p^n - 1$$

表示所有非零的互不同餘的多項式，modd p，$\varphi(x)$.

不難證明連乘積

$$\prod_\nu (X - f_\nu(x))$$

（其中 f_ν 過所有的原根）等於

$$\frac{X^{p^n-1}-1}{\prod\limits_{q}(X^{(p^n-1)/q}-1)}\quad\frac{\prod\limits_{q,q_1}(X^{(p^n-1)/qq_1}-1)}{\prod\limits_{q,q_1,q_2}(X^{(p^n-1)/qq_1q_2}-1)}\cdots,\tag{1}$$

此處 $\prod\limits_{q}$ 過 p^n-1 的所有的素因子 q，$\prod\limits_{q,q_1}$ 過 p^n-1 的所有的素因子對 q, q_1，$q\neq q_1$；等等。

習題。 證明所有的非零的互不同餘的多項式之乘積 $\equiv -1(\mathrm{modd}\,p.\ \varphi(x))$。

§11. 總結.

本章所討論之各種對象可以歸結起來，使其原則化，抽象化，因而建立起以下的各種概念。這些概念是近世代數（或稱抽象代數）之基本對象。

一組元素稱爲一集合 R。元素的個數可以是有限個，或無窮個。

1. 如其間可以定義加減，且對加減自封（卽二元素之和及差皆在此集合中），則此集合名爲模。

例如：所有的偶數成一模，所有的偶數係數的多項式也成一模。

模有時也稱爲 Abel 羣。

2. 如 R 中可以定義加減乘，且對加減乘自封，則此集合名爲環。

例如：所有的整數，所有的整係數多項式都成一環。

3. 一環 R 中之一分集 E 如適合下列二條件，則名爲理想集合：

i) 若 a, b 在 E 中，則 $a-b$ 亦在 E 中；

ii) 若 a 在 E 中而 r 在 R 中，則 ar 亦在 E 中。

例如：在所有的整數所成之環中，偶數所成之集合卽爲一理想集合。

在整係數多項式之環中，形如

$$f(x)\ (x^2+1)+2g(x)\ x$$

之多項式亦成一理想集合。此處 f 及 g 過所有的整係數多項式。

4. 如 R 中可以定義加減乘除（除數非零），而對四則運算自封，則此集合名爲域。

例如：所有的有理數成一域。

以一不可化多項式爲模，所得出的剩餘系成一域，此卽近世代數上所謂的代

數擴張.

又以素數 p 及對 p 不可化的 n 次多項式 $\varphi(x)$ 爲重模,所得出的剩餘系成一域,此域共有 p^n 個元素.

在將來學習近世代數時,如讀者能把握了本章所涉的具體例子,將幫助讀者易於捉摸其中若干概念的涵義.

第　五　章

素數分佈之概況

本章僅將素數分佈之情況，作一廣泛的敍述，而不作任何精深的探討．此可視爲解析數論之導言．本章讀者需略知微積分．

§1. 無窮大之階． 在討論素數分佈之情況時，諸無窮大之比較概況不得不知．而比較無窮大時常用次之符號：

$$\ll,\quad O,\quad o,\quad \sim .$$

今往解釋之如次：

設 n 過正整數趨向無窮（x 爲一連續變數趨向無窮）．設 $\varphi(n)$（或 $\varphi(x)$）爲 n（或 x）之正值函數，$f(n)$（或 $f(x)$）爲任一函數．若有一與 n（或 x）無關之數 A，使

$$|f| \leqslant A\varphi,$$

則吾人以

$$f \ll \varphi$$

表之．但如 $f-g\ll\varphi$，爲方便起見，吾人記之如

$$f = g + O(\varphi).$$

又 $f=o(\varphi)$，$f\sim\varphi$ 之意義各爲

$$\lim_{n\to\infty}\frac{f(n)}{\varphi(n)} = 0 \text{ 或 } 1\ \left(\text{或 } \lim_{x\to\infty}\frac{f(x)}{\varphi(x)} = 0 \text{ 或 } 1\right).$$

是以有次之數例：

$$\sin x \ll 1,\quad x+\frac{1}{x}\ll x\ll x+\frac{1}{x},\quad x+\frac{1}{x}=o(x^2),$$

$$x+\sin x\sim x,\quad \text{或}\quad x+\sin x = x+O(1).$$

當然，"趨向無窮"一語可以換作"趨於限 l"．例如當 $x\to 0$，則 $x^2=O(x)$，$\sin x\sim x$，$1+x\sim 1$ 等等．但以後如無特別聲明，則概指趨向無窮而言．

顯然有次之諸性質: (i) $\varphi \ll \varphi$; (ii) 若 $f \ll \varphi$, $\varphi \ll \psi$, 則 $f \ll \psi$; (iii) 若 $f \ll \varphi$, $g \ll \psi$, 則 $f+g \ll \varphi+\psi$ 及 $fg \ll \varphi\psi$. 如將 $\ll$ 換爲 $o(\ )$, 則 (ii) (iii) 亦眞.

又 (i) $\varphi \sim \varphi$; (ii) 若 $\psi \sim \varphi$, 則 $\varphi \sim \psi$; (iii) $\varphi \sim \psi$, $\psi \sim \chi$, 則 $\varphi \sim \chi$; (iv) 若 $\psi \sim \varphi$, $\psi_1 \sim \varphi_1$, 則 $\psi\psi_1 \sim \varphi\varphi_1$.

§ 2. **對數函數** (Logarithmic function). 於素數分佈之研究中, 對數函數 $\log x$ 實不可少. 今假定讀者已知 $\log x$ 之定義, 而重述其一二簡單性質如次: 因

$$e^x = 1 + x + \cdots + \frac{x^n}{n!} + \frac{x^{n+1}}{(n+1)!} + \cdots,$$

故當 $x \to \infty$ 時,

$$x^{-n} e^x > \frac{x}{(n+1)!},$$

而此趨向無窮. 卽 e^x 趨向無窮較 x 之任何方次爲快, 或謂 e^x 之無窮大之階大於 x^n 之階, 或可書爲 $x^n = o(e^x)$. 若 α 爲正數, 則 $x^\alpha = O(x^{[\alpha]+1}) = o(e^x)$.

因 $\log x$ 乃 e^x 之逆函數, 以 $\log y$ 代入上式之 x, 則 $(\log y)^\alpha = o(y)$. 卽得

$$\log x = o(x^\delta) \qquad (\delta > 0).$$

換言之, $\log x$ 之無窮大之階較 x 之任何正數方次爲小. 易見 $\log\log x$ 更較 $\log x$ 爲小.

定理 1.

$$\sum_{n=1}^{x} \frac{1}{n} \sim \log x.$$

證: 因

$$\log x = \int_1^x \frac{dt}{t} \leqslant \sum_{n=1}^{x} \frac{1}{n} \leqslant 1 + \int_1^x \frac{dt}{t} = 1 + \log x.$$

故得定理.

定理 2. 命

$$\mathrm{li}\, x = \lim_{\eta \to 0} \left(\int_0^{1-\eta} + \int_{1+\eta}^{x} \right) \frac{dt}{\log t},$$

則

$$\mathrm{li}\, x \sim \frac{x}{\log x}.$$

證:

$$\lim_{x\to\infty}\frac{\operatorname{li} x}{\dfrac{x}{\log x}}=\lim_{x\to\infty}\frac{(\operatorname{li} x)'}{\left(\dfrac{x}{\log x}\right)'}=$$

$$=\lim_{x\to\infty}\frac{\dfrac{1}{\log x}}{\dfrac{1}{\log x}-\dfrac{1}{\log^2 x}}=$$

$$=1.$$

§3. 引言.

素數之分佈狀況,乃數論中最有趣味之一分支. 其中之推測及定理,類多先由經驗得來. 今先將若干問題,及古人對此問題所猜測之結果,及支持此種猜測之數例,漫述如下:

(i) 命 $\pi(x)$ 爲不大於 x 之素數之個數,則有次表:

x	$\pi(x)$	$\dfrac{x}{\log x}$	$\operatorname{li} x$	$\dfrac{\pi(x)}{\operatorname{li} x}$	$\dfrac{\pi(x)}{x}$
1 000	168	145	178	0.94…	.1680
10 000	1 229	1 086	1 246	0.98…	.1229
50 000	5 133	4 621	5 167	0.993…	.1026
100 000	9 592	8 686	9 630	0.996…	.0959
500 000	41 538	38 103	41 606	0.9983…	.0830
1 000 000	78 498	72 382	78 628	0.9983…	.0785
2 000 000	148 933	137 848	149 055	0.9991…	.0745
5 000 000	348 513	324 149	348 638	0.9996…	.0697
10 000 000	664 579	620 417	664 918	0.9994…	.0665
20 000 000	1 270 607	1 189 676	1 270 905	0.9997…	.0635
90 000 000	5 216 954	4 913 897	5 217 810	0.99983…	.0580
100 000 000	5 761 455	5 428 613	5 762 209	0.99986…	.0576
1 000 000 000	50 847 478	48 254 630	50 849 235	0.99996…	.0508

此表提示吾人數點:

1) 素數之個數無窮,卽 $\pi(x)\to\infty$,

2) 但與整個之正整數之個數相比較,則所少很多. 卽 $\dfrac{\pi(x)}{x}\to 0$. 或可敍

述爲幾乎所有的整數皆非素數.

3) 素數個數之無窮大之階與 $\mathrm{li}\, x$ 十分接近,即 $\pi(x) \sim \mathrm{li}\, x \sim \frac{x}{\log x}$. 當然 3) 包有 1) 及 2).

4) $\mathrm{li}\, x$ 當爲 $\pi(x)$ 之最佳漸近式.

5) $\pi(x) < \mathrm{li}\, x$.

於本章中最深之定理爲 Чебышев 定理,即

$$\frac{x}{\log x} \ll \pi(x) \ll \frac{x}{\log x}.$$

此當然包有 1) 及 2). 而著名之素數定理 3) 將於第九章中論及之. 但 4) 之討論十分精深,不在本書範圍之內 (將於解析數論之專著中述之). 5) 並不眞實, 此點已由 Littlewood 證明之矣.

(ii) 已知

$$5, 13, 17, 29, \cdots, 10\,006\,721$$

皆爲四除餘一之素數, 因之發生一問題, 卽有此性質之素數是否無窮. 對此問題有 Dirichlet 更普遍之定理以答覆之:

若 a, b 互素,則形如 $an + b$ 之素數之個數無限.

本章僅論及此定理之若干特例. 此定理之證明見第九章.

(iii) 吾人有

$$6 = 3 + 3,\ 8 = 3 + 5,\ 10 = 5 + 5,\ 12 = 5 + 7,\ 14 = 7 + 7,\ 16 = 3 + 13,$$
$$18 = 5 + 13,\ 20 = 7 + 13,\ 22 = 3 + 19, \cdots$$

由此提示: 凡大於 4 之偶數必爲二奇素數之和,此乃著名的 Гольдбах 問題. 若此定理眞實, 則吾人可以證明: 凡大於 7 之奇數必爲三個奇素數之和. 因若 n 爲大於 7 的奇數,則 $n-3$ 乃大於 4 的偶數. 故 $n - 3 = p_1 + p_2$, 卽 $n = 3 + p_1 + p_2$.

此問題之解答,十分困難. 輓近方由蘇聯數學英雄 И. М. Виноградов 證明: 充分大之奇數,必爲三奇素數之和. 而著者曾證明: "幾乎全部"偶數皆爲二奇素數之和. 匈牙利數學家 Rényi 證明: 凡偶數 (> 2) 皆可表爲一素數與一素因數不超過定限之複合數之和.

(iv) 又

$$3, 5; 5, 7; 11, 13; 17, 19; 29, 31; \cdots; 101, 103; \cdots;$$

$$10\,016\,957, 10\,016\,959; \cdots; 10^9 + 7, 10^9 + 9; \cdots$$

皆爲差爲 2 之素數對. 更切實些, 已知小於 100 000 者有 1 224 對, 小於 1 000 000 者有 8 164 對. 目下所知最大素數對是

$$1\,000\,000\,009\,649, \quad 1\,000\,000\,009\,651.$$

此類數字資料建議: 差爲 2 之素數對可能有無窮對. 此亦一未嘗解決的問題. 切實言之, 在數論之研究中能建議之推測, 常較能解決者爲多. 又如

$$5, 7, 11; 11, 13, 17; 17, 19, 23; \cdots; 101, 103, 107;$$

$$\cdots; 10\,014\,491, 10\,014\,493, 10\,014\,497; \cdots$$

皆爲素數, 由此建議, 是否有無窮個素數 p 使 $p+2$, $p+6$ 皆爲素數. 更進一步:

(v) 已知

$$n^2 - n + 17$$

當 $0 \leqslant n \leqslant 16$ 時皆爲素數, 又

$$n^2 - n + 41$$

當 $0 \leqslant n \leqslant 40$ 時皆爲素數. 輓近 Beeger 算出

$$n^2 - n + 72491$$

當 $0 \leqslant n \leqslant 11000$ 時皆爲素數. 此建立一極有趣味之問題: 任與一數 N, 可否求出一數 p, 當 $0 \leqslant n \leqslant N$ 時, 使

$$n^2 - n + p$$

常表素數.

此亦一未解決之問題. 由著者觀之, 其困難較 (iii) 及 (iv) 更甚. 蓋若此問題已經解決, 則 (iv) 亦迎刃而解也. 何則? 多項式 $n^2 - n + p$ 最多祇當 n 由 0 到 $p-1$ 時爲素數. 今往作一系列多項式 $n^2 - n + p_i$, 具有次之性質: 當 $0 \leqslant n \leqslant p_{i-1}$ 時, $n^2 - n + p_i$ 常表素數. 故若問題 (v) 已解決, 則此種作法實爲可能. 命 $n = 1$ 及 2, 則 p_i, $p_i + 2$ 皆爲素數. 又命 $n = 1, 2, 3$, 則 p_i, $p_i + 2$, $p_i + 6$ 皆爲素數. 是以本問題如能解決, 則問題 (iv) 立刻解決.

(vi) 形如 n^2+1 之素數之個數是否無限，此亦一未解決之難題．據一般推測，其個數似應無窮：蓋已知

$$2, 5, 17, 37, \cdots, 65537, \cdots$$

等皆是也．

(vii) 命 p_n 爲第 n 個素數，p_n-p_{n-1} 之分佈情況如何？由 (iv) 已知 p_n-p_{n-1} 可能小至 2，但最大時如何？換言之，求 $\overline{\lim_{n\to\infty}}\,(p_n-p_{n-1})$ 之無窮大之階．

(viii) 有所謂 Bertrand 假定者：必有一素數在 n 與 $2n$ 之間，此乃一較易之事實，將於 §7 中證明之．更精密之推測爲“必有一素數在 n^2 與 $(n+1)^2$ 之間，此乃一未能解決之難題．

§4. 素數之個數無限．

定理 1. 素數之個數無限，卽 $\pi(x)$ 與 x 同趨向無窮．

證： 命 $2, 3, \cdots, p$ 爲不大於 p 之諸素數，又命

$$q = 2\cdot 3\cdots p + 1.$$

則 q 非 $2, 3, \cdots, p$ 之倍數，故此或爲素數，或爲 p 與 q 之間之素數所整除．故必有一大於 p 之素數存在．卽得素數之個數無限．

此一方法可用之以證明更廣泛的結果．

定理 2. 命 $f(x)$ 爲任一整係數多項式．在數列

$$f(1), f(2), f(3), \cdots$$

中包有無窮個不同的素因子．

證： 命

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n, \qquad n \geqslant 1.$$

若 $a_n=0$，則以上數列包有所有素數爲其因子，今假定 $a_n\neq 0$．

若該數列中僅有有限個素因子 $p_1, \cdots, p_\nu$．今考慮 $f(p_1\cdots p_\nu a_n y)$，此式所有的係數皆爲 a_n 之倍數，令

$$f(p_1\cdots p_\nu a_n y) = a_n g(y),$$

而

$$g(y) = 1 + A_1y + A_2y^2 + \cdots + A_ny^n$$

是一整係數多項式，且 $p_1, \cdots, p_\nu$ 整除 $A_1, A_2, \cdots, A_n$．若有一個整數 y_0 使 $g(y_0)\neq\pm 1$，則 $g(y_0)$ 中必有一素因子異於 $p_1, \cdots, p_\nu$．卽得定理．由於 $g(y)=$

± 1 最多祇能有 $2n$ 個解,故定理已完全證明矣.

對定理 1, Euler 有另一證法. 此證明方法開闢解析數論之門徑. 其方法如次:

定理 3. 級數 $\sum_p \frac{1}{p}$ 並不收斂,此處 p 過諸素數. 故素數之個數無限.

於證明此定理之前,先證

定理 4 (Euler 之恆等式). 假定 $f(n)$ 爲一函數, 對所有的正整數 n, $f(n)$ 之義確定,且並不常等於零. 若 $(n, n')=1$, 則更設

$$f(nn')=f(n)\,f(n').$$

如此則可有等式

$$\sum_{n=1}^{\infty} f(n)=\prod_p (1+f(p)+f(p^2)+\cdots);$$

此等式成立之條件爲

(i) 假定

$$\sum_{n=1}^{\infty} |f(n)|$$

收斂,或

(ii) 假定

$$\prod_p (1+|f(p)|+|f(p^2)|+\cdots)$$

收斂.

又設對諸 n 及 n' 常有 $f(nn')=f(n)\,f(n')$. 則在前之情況下,

$$\sum_{n=1}^{\infty} f(n)=\prod_p \frac{1}{1-f(p)}.$$

證: 因對諸 n 皆有

$$f(1)\,f(n)=f(n),$$

且有一 n 使 $f(n)\neq 0$. 故立得 $f(1)=1$.

1) 假定

$$\sum_{n=1}^{\infty} |f(n)| \tag{1}$$

收斂,其和爲 $\bar{S}$. 今論

$$P(x)=\prod_{p\leqslant x}(1+f(p)+f(p^2)+\cdots).$$

因對任一 p, $\sum_{n=1}^{\infty}|f(p^n)|$ 爲 (1) 中之一部,故亦收斂. 即 $P(x)$ 爲有限個絕對收斂級數之積. 故

$$P(x)=\sum{}'f(n)$$

爲一和,其中 n 過諸整數其素因子皆 $\leqslant x$ 者. 命

$$S=\sum_{n=1}^{\infty}f(n),$$

則

$$|S-P(x)|\leqslant\sum_{n>x}|f(n)|.$$

當 x 趨向無窮,則 $|S-P(x)|$ 趨向於 0, 故 $P(x)\to S$.

用此結果至函數 $|f(n)|$,則

$$\prod_p(1+|f(p)|+|f(p^2)|+\cdots)$$

收斂於 $\bar{S}$.

2) 假定

$$\prod_p(1+|f(p)|+|f(p^2)|+\cdots)$$

收斂於 $\bar{P}$. 則

$$\bar{P}(x)=\prod_{p\leqslant x}(1+|f(p)|+|f(p^2)|+\cdots)=$$

$$=\sum{}'|f(n)|\geqslant\sum_{n\leqslant x}|f(n)|.$$

故

$$\sum_{n=1}^{\infty}|f(n)|$$

收斂. 由 1) 之結果, 立得定理.

今往證明定理 2. 於上定理中取 $f(n)=\frac{1}{n}$. 若 $\sum\frac{1}{p}$ 收斂, 則由連乘積定理可知

$$\prod\left(1-\frac{1}{p}\right)\quad 及\quad \prod\left(1-\frac{1}{p}\right)^{-1}$$

收斂．由上定理可得

$$\sum_{n=1}^{\infty} \frac{1}{n}$$

亦必收斂．是不可能．故得定理．

由 $0 < 1 - \frac{1}{p} < 1$，故得:

定理 5. $\prod \left(1-\frac{1}{p}\right)$ 發散於零．

習題 1. 證明形如 $6n-1$ 之素數無限．

習題 2. 證明形如 $4n-1$ 之素數無限．

習題 3. $\frac{\pi^2}{6} = \prod_p \frac{p^2}{p^2-1}\left(\text{注意} \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}\right)$.

§5. 幾乎全部整數皆非素數．

定理 1.

$$\lim_{n\to\infty} \frac{\pi(n)}{n} = 0.$$

卽在 $1, 2, \cdots, n$ 諸整數中，其素數之個數與 n 之比接近於零．卽幾乎全部整數皆爲複合數．

證: 今將證明稍爲普遍之結果: 當 x 過實數趨向無窮，

$$\lim_{x\to\infty} \frac{\pi(x)}{x} = 0.$$

在證明之前，先說明一有用但簡單之事實: 不大於 x 之整數可爲 a 所整除者之個數爲 $\left[\frac{x}{a}\right]$．此 $[\xi]$ 表 ξ 之整數部分．

命 $\bar{\omega}(x, r)$ 表不大於 x 且不爲前 r 個素數

$$2, 3, 5, \cdots, p_r$$

所整除之整數之個數，則由定理 1.7.1，可得

$$\bar{\omega}(x, r) = [x] - \sum_{1\leqslant i\leqslant r}\left[\frac{x}{p_i}\right] + \sum_{1\leqslant i<j\leqslant r}\left[\frac{x}{p_i p_j}\right] - \cdots$$

(此式之直接證明亦不太難)．

顯然

$$\pi(x) \leqslant \bar{\omega}(x, r) + r.$$

故

$$\pi(x) < x - \sum \frac{x}{p_i} + \sum \frac{x}{p_i p_j} - \cdots + r + 2^r =$$

$$= x\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)+r+2^r <$$

$$< x\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)+2^{r+1}.$$

由定理 4.5 已知當 $r\to\infty$,

$$\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)\to 0.$$

故可取 $r=r(\epsilon)$ 使

$$\pi(x)<\frac{1}{2}\epsilon x+2^{r+1},$$

故當 x 適當大時

$$\pi(x)<\epsilon x.$$

卽得定理.

§ 6. Чебышев 定理. 本節之定理,乃初等數論中之異常重要之定理,故其證法力求純代數化.

定理 1. 當 $n\geqslant 2$, 則

$$\frac{1}{8}\leqslant \pi(n)\frac{H(n)}{n}<6,$$

此處

$$H(n)=\sum_{v=2}^{n}\frac{1}{v}.$$

卽 $\pi(n)$ 與 $\left(\frac{1}{2},\frac{1}{3},\frac{1}{4},\cdots,\frac{1}{n}\right)$ 之平均值之倒數同階.

於證此定理之前,先需下之二引:

引 1. 當 $k\geqslant 0$,

$$\pi(2^{k+1})\leqslant 2^k.$$

證: 當 $x>9$,

$$\pi(x)\leqslant\frac{x}{2},$$

此可由奇、偶數之討論知之. 又

$$\pi(2)=1=2^0,\qquad \pi(4)=2=2^1,\qquad \pi(8)=4=2^2.$$

引 2. 當 $l>0$,

$$\frac{1}{2}l\leqslant H(2^l)\leqslant l.$$

證:

$$H(2^l)=\frac{1}{2}+\left(\frac{1}{3}+\frac{1}{4}\right)+\left(\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\right)+\cdots+$$

$$+\left(\frac{1}{2^{l-1}+1}+\cdots+\frac{1}{2^l}\right)\geqslant\frac{1}{2}+\left(\frac{1}{4}+\frac{1}{4}\right)+\left(\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}\right)+$$

$$+\cdots+\left(\frac{1}{2^l}+\cdots+\frac{1}{2^l}\right)=\frac{1}{2}l.$$

$$H(2^l)=\left(\frac{1}{2}+\frac{1}{3}\right)+\left(\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}\right)+\cdots+\frac{1}{2^l}\leqslant\left(\frac{1}{2}+\frac{1}{2}\right)+$$

$$+\left(\frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}\right)+\cdots+\left(\frac{1}{2^{l-1}}+\cdots+\frac{1}{2^{l-1}}\right)+\frac{1}{2^l}\leqslant l.$$

定理之證明: 先證

$$\prod_{n<p\leqslant 2n}p\,\Big|\binom{2n}{n}=\frac{(2n)!}{n!\,n!}\Big|\prod_{p^r\leqslant 2n<p^{r+1}}p^r. \tag{1}$$

因 (i) 在 n 與 $2n$ 間之素數整除 $(2n)!$, 但不整除 $n!$, 故有上式之左. (ii) $\binom{2n}{n}$ 中 p 之方次爲

$$\sum_{m=1}^{r}\left(\left[\frac{2n}{p^m}\right]-2\left[\frac{n}{p^m}\right]\right)\leqslant r,$$

因其中之每一項皆 $\leqslant 1$. 故得 (1) 式之右邊. 由 (1) 式可知

$$n^{\pi(2n)-\pi(n)}<\prod_{n<p\leqslant 2n}p\leqslant\binom{2n}{n}\leqslant\prod_{p^r\leqslant 2n<p^{r+1}}p^r\leqslant(2n)^{\pi(2n)},\quad n\geqslant 1. \tag{2}$$

又因

$$\binom{2n}{n}=\frac{2n(2n-1)\cdots(n+1)}{n(n-1)\cdots 1}=$$

$$=2\left(2+\frac{1}{n-1}\right)\cdots\left(2+\frac{v}{n-v}\right)\cdots\left(2+\frac{n-1}{1}\right)\geqslant 2^n$$

及

$$\binom{2n}{n}\leqslant(1+1)^{2n}=2^{2n},$$

故由 (2) 可知

$$n^{\pi(2n)-\pi(n)}<2^{2n},\qquad 2^n\leqslant(2n)^{\pi(2n)},\qquad n\geqslant 1. \tag{3}$$

命 $n=2^k$, $k=0,1,2,\cdots$, 可得

$$2^{k(\pi(2^{k+1})-\pi(2^k))} < 2^{2^{k+1}}, \qquad 2^{2^k} \leqslant 2^{(k+1)\pi(2^{k+1})}, \qquad k \geqslant 0,$$

卽得

$$k(\pi(2^{k+1}) - \pi(2^k)) < 2^{k+1}, \qquad 2^k \leqslant (k+1)\pi(2^{k+1}). \tag{4}$$

由引 1,

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) < 2^{k+1} + \pi(2^{k+1}) \leqslant 3\cdot 2^k, \qquad k \geqslant 0,$$

令 $k = 0, 1, \cdots, k$, 而將所得之諸式相加,得

$$(k+1)\pi(2^{k+1}) < 3(2^0 + 2^1 + \cdots + 2^k) < 3\cdot 2^{k+1}, \qquad k \geqslant 0. \tag{5}$$

由 (4) 及 (5) 可知

$$\frac{1}{2}\frac{2^{k+1}}{k+1} \leqslant \pi(2^{k+1}) < 3\frac{2^{k+1}}{k+1}, \qquad k \geqslant 0. \tag{6}$$

命 n 爲 $\geqslant 2$ 之整數,取 k 使

$$2^{k+1} \leqslant n < 2^{k+2}, \qquad k \geqslant 0.$$

由引 2,

$$\pi(n) \leqslant \pi(2^{k+2}) < 3\frac{2^{k+2}}{k+2} \leqslant 6\frac{2^{k+1}}{H(2^{k+2})} \leqslant 6\frac{n}{H(n)}, \tag{7}$$

及

$$\pi(n) \geqslant \pi(2^{k+1}) \geqslant \frac{1}{2}\frac{2^{k+1}}{k+1} = \frac{1}{8}\frac{2^{k+2}}{\frac{1}{2}(k+1)} \geqslant$$

$$\geqslant \frac{1}{8}\frac{2^{k+2}}{H(2^{k+1})} \geqslant \frac{1}{8}\frac{n}{H(n)}. \tag{8}$$

此對 $n \geqslant 2$ 皆眞. 故

$$\frac{1}{8} \leqslant \pi(n)\frac{H(n)}{n} < 6.$$

定理 2. 當 $n \geqslant 2$,

$$\frac{1}{8} \leqslant \frac{\pi(n)}{\frac{n}{\log n}} \leqslant 12.$$

證: 當 $n \geqslant 2$,

$$\log\frac{n}{2} = \int_2^n \frac{dt}{t} < \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} < \int_1^n \frac{dt}{t} = \log n.$$

當 $n \geqslant 4$,

$$\log\frac{n}{2} \geqslant \frac{1}{2}\log n.$$

又

$$\frac{1}{2}\log 3 \leqslant \frac{1}{2}+\frac{1}{3},$$

$$\frac{1}{2}\log 2 \leqslant \frac{1}{2},$$

故得定理.

顯然定理 4.1 及定理 5.1 都可由此定理推出.

§ 7. **Bertrand 假設.**

Bertrand 假設之證明乃 Чебышев 所首先獲得.

定理 1. 對任一實數 $x \geqslant 1$, 在 x 及 $2x$ 之間必有一素數.

證: 1) 仍由二項式係數

$$\binom{2n}{n}=\frac{(2n)!}{n!\,n!}$$

出發. 但需要更精密的估計: 當 $n \geqslant 5$ 時,

$$\frac{1}{2n}2^{2n}<\binom{2n}{n}<\frac{1}{4}2^{2n}. \tag{1}$$

此式之左邊之證明如次:

$$(2n)\binom{2n}{n}=\frac{2}{1}\cdot\frac{3}{1}\cdot\frac{4}{2}\cdot\frac{5}{2}\cdots\frac{2n-2}{n-1}\,\frac{2n-1}{n-1}\,\frac{2n}{n}\,\frac{2n}{n}>2^{2n},$$

而右邊則用歸納法. 當 $n=5$ 時顯然有

$$\binom{2n}{n}=252<256=\frac{1}{4}\cdot 2^{10}.$$

由於

$$\binom{2(n+1)}{n+1}=\frac{(2n)!\,(2n+1)\,(2n+2)}{(n!)^2\,(n+1)\,(n+1)}<4\binom{2n}{n},$$

而得所需.

2) 命 $b \geqslant 10$. 以 $\{\xi\}$ 表 $\geqslant \xi$ 之最小之整數, 且命

$$a_1=\left\{\frac{b}{2}\right\},\quad a_2=\left\{\frac{b}{2^2}\right\},\cdots,\quad a_k=\left\{\frac{b}{2^k}\right\},\cdots.$$

如此則

$$a_1 \geqslant a_2 \geqslant \cdots \geqslant a_k \geqslant \cdots,$$

及

$$a_k < \frac{b}{2^k} + 1 = 2\,\frac{b}{2^{k+1}} + 1 \leqslant 2\,a_{k+1} + 1 .$$

由於兩邊都是整數,故得

$$a_k \leqslant 2\,a_{k+1} . \tag{2}$$

命 m 爲最大之整數使得 $a_m \geqslant 5$ 者. 卽 $a_{m+1} < 5$. 又由 (2) 式, $a_m < 10$. 因 $2\,a_1 \geqslant b$, 故 m 個隔間

$$a_m < \eta \leqslant 2\,a_m,\quad a_{m-1} < \eta \leqslant 2\,a_{m-1}, \cdots,\quad a_1 < \eta \leqslant 2\,a_1$$

整個地掩蓋了隔間 $10 < \eta \leqslant b$. 故

$$\prod_{10<p\leqslant b} p \leqslant \prod_{a_1<p\leqslant 2a_1} p \prod_{a_2<p\leqslant 2a_2} p \cdots \prod_{a_m<p\leqslant 2a_m} p .$$

由於

$$\prod_{n<p\leqslant 2n} p < \binom{2n}{n} < 2^{2(n-1)},$$

可知

$$\prod_{10<p\leqslant b} p \leqslant 2^{2(a_1-1+a_2-1+\cdots+a_m-1)} <$$

$$< 2^{2\left(\frac{b}{2}+\frac{b}{2^2}+\cdots+\frac{b}{2^m}\right)} < 2^{2b}, \tag{3}$$

3) 在上定理中已經證明: 一素數 p 在 $\binom{2n}{n}$ 中之冪數不大於 r, 此 r 乃最大之整數使 $p^r \leqslant 2n$ 者. 由此可知素數 p 之大於 $\sqrt{2n}$ 者其平方必不能整除 $\binom{2n}{n}$.

尤可注意者,當 $n \geqslant 3$ 時,適合於 $\frac{2}{3}n < p \leqslant n$ 之素數 p 不能整除 $\binom{2n}{n}$. 蓋 $3p > 2n$, 故在 $(2n)!$ 之諸因子中僅有 p 及 $2p$ 出現, 而無其他之 p 的倍數. 而 $(n!)^2$ 中顯然有因子 p^2. 故如此之 p 不能整除 $\binom{2n}{n}$. (此乃本證明中最主要之點.)

總括以上所述,

$$\binom{2n}{n} \leqslant \prod_{p\leqslant\sqrt{2n}} p^r \prod_{\sqrt{2n}<p\leqslant\frac{2}{3}n} p \prod_{n<p\leqslant 2n} p \leqslant$$

$$\leqslant \prod_{p\leqslant\sqrt{2n}} (2n) \prod_{\sqrt{2n}<p\leqslant\frac{2}{3}n} p \prod_{n<p\leqslant 2n} p .$$

由 (1) 及 (3) 可知,當 $n \geqslant 50$ 時 (卽 $\sqrt{2n} \geqslant 10$ 時),

$$2^{2n} < (2n)^{\sqrt{2n}+1} \prod_{\sqrt{2n}<p\leqslant\frac{2}{3}n} p \prod_{n<p\leqslant 2n} p <$$

$$< (2n)^{\sqrt{2n}+1}\, 2^{\frac{4}{3}n} \prod_{n<p\leqslant 2n} p. \tag{4}$$

若在 n 及 $2n$ 間並無素數,則得

$$2^{2n} < (2n)^{\sqrt{2n}+1}\, 2^{\frac{4}{3}n},$$

卽

$$2^{\frac{2}{3}n} < (2n)^{\sqrt{2n}+1}. \tag{5}$$

當 n 充分大時,此式顯然不可能. 今更具體地算出此式成立之確切範圍. 今用不等式 $n \leqslant 2^{n-1}$ (此式可用歸納法證之),

$$2n = (\sqrt[6]{2n})^6 < ([\sqrt[6]{2n}]+1)^6 \leqslant 2^{6[\sqrt[6]{2n}]} \leqslant 2^{6\sqrt[6]{2n}}, \tag{6}$$

由 (5) 可知 (仍假定 $n \geqslant 50$)

$$2^{2n} < (2n)^{3(1+\sqrt{2n})} < 2^{\sqrt[6]{2n}\,(18+18\sqrt{2n})} < 2^{\sqrt[6]{2n}\times 20\sqrt{2n}} = 2^{20(2n)^{\frac{2}{3}}},$$

卽 $(2n)^{\frac{1}{3}} < 20$, $n < \frac{1}{2}\cdot 20^3 = 4000$. 卽 (5) 式僅當 $n < 4000$ 時可能成立. 故當 $n \geqslant 4000$ 時必有一素數 p 適合於 $n < p \leqslant 2n$.

4) 當 $n < 4000$ 時可以證之如次:

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001 \tag{7}$$

乃一連串素數,後者小於前者之二倍,對任一 n $(1 \leqslant n < 4000)$ 可於 (7) 中取得一最小素數 p 而大於 n 者. 命 p' 爲其前一項,則

$$p' \leqslant n < p \leqslant 2p' \leqslant 2n.$$

故得定理 1.

定理 2. 當 $n \geqslant 1$, 則有二正常數 α 及 β 使

$$\alpha\frac{n}{\log n} < \pi(2n) - \pi(n) < \beta\frac{n}{\log n}.$$

證: 此式之右邊可由上節之定理立刻推得.

由 (4) 式可知 (並利用 (6) 式),當 $n \geqslant 4000$ ($n < 4000$ 時,定理顯然),

$$\prod_{n<p\leqslant 2n} p > 2^{2n-\frac{4}{3}n}(2n)^{-(1+\sqrt{2n})} >$$

$$> 2^{\frac{1}{3}(2n-\sqrt[6]{2n}(18+18\sqrt{2n}))} >$$

$$> 2^{\frac{1}{3}(2n-19(2n)^{\frac{2}{3}})} \geqslant$$

$$\geqslant 2^{\frac{2}{3}n(1-19/20)} = 2^{\frac{1}{30}n}.$$

由於

$$\prod_{n<p\leqslant 2n} p < (2n)^{\pi(2n)-\pi(n)},$$

可知

$$\pi(2n)-\pi(n) > \frac{\log 2}{30}\cdot\frac{n}{\log 2n},$$

故得定理.

附記: 按定理 1 之性質,就一方面而言,固已解決 Bertrand 所推測之難題.但就另一方面言,此定理之精確性並不算好,蓋有遠較此定理更精確之結果存在,惟超出本書範疇不能敍述耳.

習題. 試用微積分方法計算 (5) 成立之界限.

§ 8. 以積分來估計和之數值.

定理 1. 若 $x \geqslant a$ 時,$f(x)$ 是一遞增非負函數,則當 $\xi \geqslant a$ 時常有

$$\left|\sum_{a\leqslant n\leqslant\xi} f(n) - \int_a^{\xi} f(x)\,dx\right| \leqslant f(\xi).$$

證: 取 $[\xi] = b$. 則

$$\int_a^b f(x)\,dx = \sum_{i=a}^{b-1}\int_i^{i+1} f(x)\,dx \begin{cases} \geqslant \sum_{i=a}^{b-1} f(i) \\ \leqslant \sum_{i=a}^{b-1} f(i+1), \end{cases}$$

即

$$f(a)+\cdots+f(b-1) \leqslant \int_a^b f(x)\,dx \leqslant f(a+1)+\cdots+f(b);$$

又

$$0 \leqslant \int_b^{\xi} f(x)\,dx \leqslant f(\xi),$$

併之可得定理.

例 1. 命 $\lambda\geqslant 0$, $f(x)=x^{\lambda}$, 則得

$$\left|\sum_{a\leqslant n\leqslant \xi} n^{\lambda}-\frac{\xi^{\lambda+1}-a^{\lambda+1}}{\lambda+1}\right|\leqslant \xi^{\lambda}.$$

由例 1 可知,當 $\lambda\geqslant 0$ 時,

$$\sum_{1\leqslant n\leqslant \xi} n^{\lambda}=\frac{\xi^{\lambda+1}}{\lambda+1}+O(\xi^{\lambda}). \tag{1}$$

由此也可得出

$$\sum_{1\leqslant n\leqslant \xi} n^{\lambda}=O(\xi^{\lambda+1}).$$

例 2. 命 $f(x)=\log x$, $\xi\geqslant 1$ 及 $T(\xi)=\sum_{n\leqslant \xi}\log n$, 則得

$$|T(\xi)-\int_1^{\xi}\log x\,dx|\leqslant \log \xi,$$

即

$$|T(\xi)-\xi\log\xi+\xi-1|\leqslant \log\xi. \tag{2}$$

特別當 ξ 爲整數 n 時,則

$$n\log n-n+1-\log n\leqslant \log n!\leqslant n\log n-n+1+\log n,$$

即

$$n^{n-1}e^{-n+1}\leqslant n!\leqslant n^{n+1}e^{-n+1}. \tag{3}$$

習題 1. 設 ξ 是整數,在 (1) 式中多求一項,即當 $\lambda\geqslant 1$ 時,定出 c 使

$$\sum_{1\leqslant n\leqslant \xi} n^{\lambda}=\frac{\xi^{\lambda+1}}{\lambda+1}+c\,\xi^{\lambda}+O(\xi^{\lambda-1}).$$

習題 2. 引用定理 1 以研究和

$$\sum_{3\leqslant n\leqslant \xi}\log\log n.$$

關於遞減函數有以下結果:

定理 2. 設 $x\geqslant a$ 時, $f(x)$ 是一非負的遞減函數, 則極限

$$\lim_{N\to\infty}\left(\sum_{n=a}^{N} f(n)-\int_a^N f(x)\,dx\right)=\alpha \tag{4}$$

存在,且 $0\leqslant\alpha\leqslant f(a)$. 更進一步言之, 當 $x\to\infty$ 時,若 $f(x)\to 0$, 則

$$\left|\sum_{a\leqslant n\leqslant\xi} f(n)-\int_a^\xi f(v)\,dv-\alpha\right|\leqslant f(\xi-1),\qquad (若\ \xi\geqslant a+1). \tag{5}$$

證：命

$$g(\xi)=\sum_{a\leqslant n\leqslant\xi} f(n)-\int_a^\xi f(x)\,dx,$$

則

$$g(n)-g(n+1)=-f(n+1)+\int_n^{n+1} f(x)\,dx\geqslant$$
$$\geqslant -f(n+1)+f(n+1)=0.$$

又

$$g(N)=\sum_{n=a}^{N-1}\left(f(n)-\int_n^{n+1} f(x)\,dx\right)+f(N)\geqslant$$
$$\geqslant\sum_{n=a}^{N-1}(f(n)-f(n))+f(N)=f(N)\geqslant 0,$$

故 $g(n)$ 爲一遞減函數，且

$$0\leqslant g(n)\leqslant g(a)=f(a).$$

故 $g(n)$ 之極限存在，命之爲 α，且 $0\leqslant\alpha\leqslant f(a)$.

今更假定當 $x\to\infty$ 時，$f(x)\to 0$，則

$$g(\xi)-\alpha=\sum_{a\leqslant n\leqslant\xi} f(n)-\int_a^\xi f(x)\,dx-\lim_{N\to\infty}\left(\sum_{n=a}^N f(n)-\int_a^N f(x)\,dx\right)=$$
$$=\sum_{n=a}^{[\xi]} f(n)-\int_a^{[\xi]} f(x)\,dx-\int_{[\xi]}^\xi f(x)\,dx-$$
$$-\lim_{N\to\infty}\left(\sum_{n=a}^N f(n)-\int_a^N f(x)\,dx\right)=$$
$$=-\int_{[\xi]}^\xi f(x)\,dx-\lim_{N\to\infty}\left(\sum_{n=[\xi]+1}^N f(n)-\int_{[\xi]}^N f(x)\,dx\right)=$$
$$=-\int_{[\xi]}^\xi f(x)\,dx+\lim_{N\to\infty}\sum_{n=[\xi]+1}^N\int_{n-1}^n (f(x)-f(n))\,dx$$

$$\begin{cases}\leqslant\lim\limits_{N\to\infty}\sum\limits_{n=[\xi]+1}^N\int_{n-1}^n (f(n-1)-f(n))\,dx=f([\xi])\leqslant f(\xi-1),\\ \geqslant-\int_{[\xi]}^\xi f(x)\,dx\geqslant-(\xi-[\xi])\,f([\xi])\geqslant-f(\xi-1),\end{cases}$$

故得定理.

例 3. 取 $a=1$, $f(x)=\frac{1}{x}$. 此時 α 名爲 Euler 常數以 γ 表之. 故得 $0\leqslant\gamma\leqslant 1$, 且

$$\sum_{1\leqslant n\leqslant\xi}\frac{1}{n}=\log\xi+\gamma+O\left(\frac{1}{\xi}\right). \tag{6}$$

例 4. 命 $0<\sigma\neq 1$. $f(x)=x^{-\sigma}$, 則有一常數 $\alpha=\alpha\ (a,\sigma)$ 依於 a 及 σ, 使當 $a\geqslant 1$ 時,有

$$\left|\sum_{a\leqslant n\leqslant\xi}\frac{1}{n^\sigma}-\frac{\xi^{1-\sigma}-a^{1-\sigma}}{1-\sigma}-\alpha\right|\leqslant\frac{1}{(\xi-1)^\sigma}. \tag{7}$$

由此獲得: 若 $\sigma>1$, 級數

$$\sum_{n=1}^{\infty}\frac{1}{n^\sigma}$$

收斂,且當 $\xi\geqslant 1$ 時

$$\sum_{n>\xi}\frac{1}{n^\sigma}=\frac{1}{(\sigma-1)\,\xi^{\sigma-1}}+O\left(\frac{1}{\xi^\sigma}\right). \tag{8}$$

(1),(3),(6),(8) 四式經常用到,讀者最好加以熟記.

習題 1. 證明當 $\xi\geqslant 2$ 時

$$\sum_{1\leqslant n\leqslant\xi}\frac{\log n}{n}=\frac{1}{2}\log^2\xi+c_1+O\left(\frac{\log\xi}{\xi}\right).$$

習題 2. 證明當 $\xi\geqslant 2$ 時

$$\sum_{2\leqslant n\leqslant\xi}\frac{1}{n\log n}=\log\log\xi+c_2+O\left(\frac{1}{\xi\log\xi}\right).$$

§9. Чебышев 定理之推論.

本節中所用之 $c_1, c_2, \cdots$ 皆絕對常數.

定理 1. 當 $\xi\geqslant 1$ 時,有一常數 c_1 使

$$\left|\sum_{p\leqslant\xi}\frac{\log p}{p}-\log\xi\right|<c_1.$$

此處 $\sum\limits_{p\leqslant\xi}$ 表示和中之 p 過所有不大於 ξ 之素數.

證: 1) 先設 $\xi=x$ 爲整數. 由定理 1.11.1,

$$T(x)=\log x!=\log\prod_{p\leqslant x}p^{\left[\frac{x}{p}\right]+\left[\frac{x}{p^2}\right]+\cdots}=\sum_{p\leqslant x}\left(\left[\frac{x}{p}\right]+\left[\frac{x}{p^2}\right]+\cdots\right)\log p.$$

由

$$\frac{x}{p}-1<\left[\frac{x}{p}\right]+\left[\frac{x}{p^2}\right]+\cdots\leqslant\frac{x}{p}+\frac{x}{p^2}+\cdots\leqslant\frac{x}{p}+\frac{x}{p(p-1)},$$

可得

$$\sum_{p\leqslant x}\frac{x\log p}{p}-\sum_{p\leqslant x}\log p<T(x)\leqslant x\left(\sum_{p\leqslant x}\frac{\log p}{p}+\sum_{p\leqslant x}\frac{\log p}{p(p-1)}\right).\quad(1)$$

由定理 6.2，

$$\sum_{p\leqslant x}\log p\leqslant\log x\,\pi(x)\leqslant c_2x$$

及

$$\sum_{p\leqslant x}\frac{\log p}{p(p-1)}\leqslant\sum_{2\leqslant n\leqslant x+1}\frac{\log n}{(n-1)^2}\leqslant\sum_{n=1}^{\infty}\frac{\log(n+1)}{n^2}=c_3,$$

代入 (1) 式得

$$\left|T(x)-x\sum_{p\leqslant x}\frac{\log p}{p}\right|\leqslant c_4x.$$

由例 8.2 得

$$|T(x)-x\log x|<c_5x.$$

但

$$\left|x\sum_{p\leqslant x}\frac{\log p}{p}-x\log x\right|\leqslant\left|T(x)-x\sum_{p\leqslant x}\frac{\log p}{p}\right|+\left|T(x)-x\log x\right|<$$
$$<c_4x+c_5x=c_6x,$$

故得

$$\left|\sum_{p\leqslant x}\frac{\log p}{p}-\log x\right|<c_6.$$

2) 設 ξ 爲任意實數,則

$$\sum_{p\leqslant\xi}\frac{\log p}{p}=\sum_{p\leqslant[\xi]}\frac{\log p}{p}.$$

由適所證出之結果得

$$\left|\sum_{p\leqslant\xi}\frac{\log p}{p}-\log[\xi]\right|<c_6.$$

但

$$|\log[\xi]-\log\xi| = \int_{[\xi]}^{\xi} d(\log t) = \int_{[\xi]}^{\xi} \frac{dt}{t} \leqslant \int_{[\xi]}^{\xi} dt \leqslant 1,$$

故有

$$\left|\sum_{p\leqslant\xi}\frac{\log p}{p}-\log\xi\right| < c_6+1=c_1.$$

故定理完全證明.

定理 2. 設 $\xi\geqslant 2$, 有一常數 c_7 使

$$\sum_{p\leqslant\xi}\frac{1}{p}=\log\log\xi+c_7+O\left(\frac{1}{\log\xi}\right).$$

證: 命

$$S(n)=\sum_{p\leqslant n}\frac{\log p}{p}.$$

由定理 1,

$$S(n)=\log n+r_n,\qquad r_n=O(1).$$

故

$$\sum_{p\leqslant\xi}\frac{1}{p}=\sum_{p\leqslant\xi}\frac{\log p}{p}\cdot\frac{1}{\log p}=\sum_{2\leqslant n\leqslant\xi}\frac{S(n)-S(n-1)}{\log n}=$$

$$=\sum_{2\leqslant n\leqslant\xi}\frac{\log n-\log(n-1)}{\log n}+\sum_{2\leqslant n\leqslant\xi}\frac{r_n-r_{n-1}}{\log n}=\sum{}_1+\sum{}_2. \qquad (2)$$

由於 $x\geqslant 2$ 時, $f(x)=-\dfrac{\log\left(1-\frac{1}{x}\right)}{\log x}$ 是遞減函數, 且當 $x\to\infty$ 時, $f(x)\to 0$. 故由定理 8.2 得

$$\sum{}_1=-\sum_{2\leqslant n\leqslant\xi}\frac{\log\left(1-\frac{1}{n}\right)}{\log n}=-\int_2^{\xi}\frac{\log\left(1-\frac{1}{x}\right)}{\log x}dx+c_8+O(f(\xi)).$$

由於

$$f(x)=\frac{1}{x\log x}+O\left(\frac{1}{x^2\log x}\right),$$

故積分

$$\int_2^{\infty}\frac{-\log\left(1-\frac{1}{x}\right)-\frac{1}{x}}{\log x}dx$$

收斂,設其值為 c_9, 則

$$\sum\nolimits_1 = \int_2^\xi \frac{dx}{x\log x} + c_8 + \int_2^\xi \frac{-\log\left(1-\frac{1}{x}\right)-\frac{1}{x}}{\log x}dx + O\left(\frac{1}{\xi\log\xi}\right) =$$

$$= \log\log\xi - \log\log 2 + c_8 + c_9 + \int_\xi^\infty \frac{\log\left(1-\frac{1}{x}\right)+\frac{1}{x}}{\log x}dx +$$

$$+ O\left(\frac{1}{\xi\log\xi}\right) = \log\log\xi + c_{10} + O\left(\frac{1}{\xi\log\xi}\right), \tag{3}$$

此處用到$\int_\xi^\infty \frac{\log\left(1-\frac{1}{x}\right)+\frac{1}{x}}{\log\ x} = O\left(\int_\xi^\infty \frac{dx}{x^2\log x}\right) = O\left(\frac{1}{\log\xi}\int_\xi^\infty\frac{dx}{x^2}\right) = O\left(\frac{1}{\xi\log\xi}\right)$.

又由於 $r_n = O(1)$ 及 $\sum_{n=2}^\infty\left(\frac{1}{\log n} - \frac{1}{\log(n+1)}\right)$ 爲正項收斂級數,故級數

$$\sum_{n=2}^\infty r_n\left(\frac{1}{\log n} - \frac{1}{\log(n+1)}\right)$$

收斂,設其值爲 c_{11}. 又

$$\sum_{n>\xi} r_n\left(\frac{1}{\log n} - \frac{1}{\log(n+1)}\right) = O\left(\sum_{n>\xi}\left|\frac{1}{\log n} - \frac{1}{\log(n+1)}\right|\right) =$$

$$= O\left(\sum_{n>\xi}\frac{1}{n\log^2 n}\right) = O\left(\frac{1}{\log\xi}\right).$$

故

$$\sum\nolimits_2 = \sum_{2\leqslant n\leqslant\xi} r_n\left(\frac{1}{\log n} - \frac{1}{\log(n+1)}\right) + O\left(\frac{r_\xi}{\log\xi}\right) =$$

$$= \sum_{n=2}^\infty r_n\left(\frac{1}{\log n} - \frac{1}{\log(n+1)}\right) - \sum_{n>\xi} r_n\left(\frac{1}{\log n} - \frac{1}{\log(n+1)}\right) +$$

$$+ O\left(\frac{1}{\log\xi}\right) = c_{11} + O\left(\frac{1}{\log\xi}\right). \tag{4}$$

由 (2), (3), (4) 得

$$\sum_{p\leqslant\xi}\frac{1}{p} = \log\log\xi + c_{10} + c_{11} + O\left(\frac{1}{\log\xi}\right) =$$

$$= \log\log\xi + c_7 + O\left(\frac{1}{\log\xi}\right).$$

定理證完.

定理 3. 設 $\xi \geqslant 2$. 有一常數 c_{12} 使

$$\prod_{p\leqslant\xi}\left(1-\frac{1}{p}\right)=\frac{c_{12}}{\log\xi}+O\left(\frac{1}{\log^2\xi}\right).$$

證: 由於

$$\sum_{p>\xi}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)=O\left(\sum_{p>\xi}\frac{1}{p^2}\right)=O\left(\sum_{n>\xi}\frac{1}{n^2}\right)=O\left(\frac{1}{\xi}\right),$$

故由適所證之定理得

$$\log\prod_{p\leqslant\xi}\left(1-\frac{1}{p}\right)=\sum_{p\leqslant\xi}\log\left(1-\frac{1}{p}\right)=-\sum_{p\leqslant\xi}\frac{1}{p}+\sum_{p\leqslant\xi}\left[\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right]=$$

$$=-\log\log\xi-c_7+O\left(\frac{1}{\log\xi}\right)+\sum_{p>2}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)-$$

$$-\sum_{p>\xi}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)=-\log\log\xi+c_{13}+O\left(\frac{1}{\log\xi}\right),$$

此處

$$c_{13}=-c_7+\sum_{p>2}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right).$$

故

$$\prod_{p\leqslant\xi}\left(1-\frac{1}{p}\right)=e^{-\log\log\xi+c_{13}+O\left(\frac{1}{\log\xi}\right)}=\frac{e^{c_{13}}}{\log\xi}\cdot e^{O\left(\frac{1}{\log\xi}\right)}=$$

$$=\frac{c_{12}}{\log\xi}\left(1+O\left(\frac{1}{\log\xi}\right)\right)\quad(c_{12}=e^{c_{13}}),$$

此處用到 $e^{O\left(\frac{1}{\log\xi}\right)}=1+O\left(\frac{1}{\log\xi}\right)$.

定理證完.

定理 2 及 3 較定理 4.3 及 4.5 為精密.

習題 1. 設 p_n 表示第 n 個素數,則存在正常數 c_1, c_2, 使

$$c_1 n\log n<p_n<c_2 n\log n.$$

習題 2. 存在正常數 c, 使

$$\varphi(n)>c\frac{n}{\log\log n}\qquad(n\geqslant 3).$$

習題 3. 試證無窮級數

$$\sum_p\frac{1}{p(\log\log p)^h}$$

當 $h>1$ 時收斂,當 $h\leqslant 1$ 時發散,此處 $\sum_p$ 表示通過所有的素數.

§ 10. n 之素因子的個數.

命 n 為一正整數, $\omega(n)$ 表 n 之不同素因子的個數, $\Omega(n)$ 表 n 之全部素因子的個數. 即若 $n=p_1^{a_1}\cdots p_s^{a_s}$, 則

$$\omega(n)=s,\qquad \Omega(n)=a_1+\cdots+a_s. \tag{1}$$

當 n 為素數時,

$$\omega(n)=\Omega(n)=1;$$

但當 n 通過 2 之乘方而趨於無窮時.

$$\Omega(n)=\frac{\log n}{\log 2}\to\infty;$$

當 n 通過素數之連乘積, $n=p_1p_2\cdots p_s$, 而趨於無窮時,

$$\omega(n)=s\to\infty.$$

故 $\omega(n)$ 與 $\Omega(n)$ 之值是很不規律的,吾人不能獲得其漸近公式. 但吾人有下之定理:

定理 1.

$$\sum_{n\leqslant x}\omega(n)=x\log\log x+c_1x+o(x), \tag{2}$$

$$\sum_{n\leqslant x}\Omega(n)=x\log\log x+c_2x+o(x), \tag{3}$$

此處 c_1, c_2 是正常數.

證: 1) 吾人有

$$\sum_{n\leqslant x}\omega(n)=\sum_{n\leqslant x}\sum_{p\mid n}1=\sum_{p\leqslant x}\left[\frac{x}{p}\right]=\sum_{p\leqslant x}\frac{x}{p}+O(\pi(x)).$$

由定理 9.2 及 6.2 即得 (2) 式.

2) 又

$$\sum_{n\leqslant x}\Omega(n)=\sum_{n\leqslant x}\sum_{p^m\mid n}1=\sum_{p^m\leqslant x}\left[\frac{x}{p^m}\right]=\sum_{p\leqslant x}\left[\frac{x}{p}\right]+\sum_{\substack{p^m\leqslant x\\ m\geqslant 2}}\left[\frac{x}{p^m}\right],$$

由定理 6.2,

$$\sum_{\substack{p^m\leqslant x\\ m\geqslant 2}} 1 \leqslant \sum_{p^2\leqslant x} 1 + \sum_{p^3\leqslant x} 1 + \cdots + \sum_{p^{\left[\frac{\log x}{\log 2}\right]}\leqslant x} 1 \leqslant \frac{\log x}{\log 2}\sum_{p^2\leqslant x} 1 = \frac{\log x}{\log 2}\pi(\sqrt{x}) = o(x).$$

故

$$\sum_{n\leqslant x}\Omega(n) = \sum_{n\leqslant x}\omega(n) + \sum_{\substack{p^m\leqslant x\\ m\geqslant 2}}\frac{x}{p^m} + o(x).$$

但級數

$$\sum_{m=2}^{\infty}\sum_{p}\frac{1}{p^m} = \sum_{p}\left(\frac{1}{p^2}+\frac{1}{p^3}+\cdots\right) = \sum_{p}\frac{1}{p(p-1)} = c$$

是收斂的，故得

$$\sum_{n\leqslant x}\Omega(n) = \sum_{n\leqslant x}\omega(n) + x(c+o(1)) + o(x) = x\log\log x + c_2 x + o(x).$$

定理 2. **(Hardy-Ramanujan).** 若以 $f(n)$ 表 $\omega(n)$ 或 $\Omega(n)$，則對任一 $\varepsilon > 0$，使

$$|f(n) - \log\log n| > (\log\log n)^{\frac{1}{2}+\varepsilon} \tag{4}$$

之不超過 x 的 n 的個數爲 $o(x)$.

證 (Turán)： 因當 $x^{\frac{1}{e}} < n \leqslant x$ 時

$$\log\log x - 1 < \log\log n \leqslant \log\log x,$$

而 $\leqslant x^{\frac{1}{e}}$ 的 n 的個數

$$[x^{\frac{1}{e}}] = o(x),$$

故祇須證明使

$$|f(n) - \log\log x| > (\log\log x)^{\frac{1}{2}+\varepsilon} \tag{5}$$

之 n $(\leqslant x)$ 之個數爲 $o(x)$ 卽足.

又由於 $\Omega(n) \geqslant \omega(n)$；又由 (2) 及 (3)，

$$\sum_{n\leqslant x}(\Omega(n) - \omega(n)) = O(x),$$

因此使

$$\Omega(n) - \omega(n) > (\log\log x)^{\frac{1}{2}}$$

之 n $(\leqslant x)$ 之個數爲

$$O\left(\frac{x}{(\log\log x)^{1/2}}\right) = o(x).$$

故祇須就 $f(n)=\omega(n)$ 之情況證明之卽足.

考慮 n 之不同素因子對 p, q, ($p\neq q$, p,q 與 q,p 算作不同的兩對), p 可以取 $\omega(n)$ 個値,對每一固定之 p, q 可以取 $\omega(n)-1$ 個値,故得

$$\omega(n)(\omega(n)-1)=\sum_{\substack{pq\mid n\\ p\neq q}}1=\sum_{pq\mid n}1-\sum_{p^2\mid n}1.$$

就 $n=1,2,\cdots,[x]$ 加之, 得

$$\sum_{n\leqslant x}\omega^2(n)-\sum_{n\leqslant x}\omega(n)=\sum_{n\leqslant x}\Big(\sum_{pq\mid n}1-\sum_{p^2\mid n}1\Big)=\sum_{pq\leqslant x}\left[\frac{x}{pq}\right]-\sum_{p^2\leqslant x}\left[\frac{x}{p^2}\right]. \quad (6)$$

因

$$\sum_{p^2\leqslant x}\left[\frac{x}{p^2}\right]\leqslant\sum_{p^2\leqslant x}\frac{x}{p^2}\leqslant x\sum_{p}\frac{1}{p^2}=O(x)$$

及

$$\sum_{pq\leqslant x}\left[\frac{x}{pq}\right]=x\sum_{pq\leqslant x}\frac{1}{pq}+O(x),$$

故由 (2) 及 (6) 得

$$\sum_{n\leqslant x}\omega^2(n)=x\sum_{pq\leqslant x}\frac{1}{pq}+O(x\log\log x). \quad (7)$$

今

$$\Big(\sum_{p\leqslant\sqrt{x}}\frac{1}{p}\Big)^2\leqslant\sum_{pq\leqslant x}\frac{1}{pq}\leqslant\Big(\sum_{p\leqslant x}\frac{1}{p}\Big)^2,$$

由於 $\sum_{p\leqslant\xi}\frac{1}{p}=\log\log\xi+O(1)$, 故上式兩端都等於

$$(\log\log x+O(1))^2=(\log\log x)^2+O(\log\log x).$$

故由 (7) 得

$$\sum_{n\leqslant x}\omega^2(n)=x(\log\log x)^2+O(x\log\log x). \quad (8)$$

由是

$$\sum_{n\leqslant x}(\omega(n)-\log\log x)^2=\sum_{n\leqslant x}\omega^2(n)-2\log\log x\sum_{n\leqslant x}\omega(n)+[x](\log\log x)^2=$$
$$=x(\log\log x)^2+O(x\log\log x)-2\log\log x(x\log\log x+O(x))+$$
$$+(x+O(1))(\log\log x)^2=O(x\log\log x). \quad (9)$$

對任一 $\delta>0$, 若有 δx 個不超過 x 之正整數使 (5) 式成立,則有

$$\sum_{n\leqslant x}(\omega(n)-\log\log x)^2\geqslant\delta x(\log\log x)^{1+2\varepsilon}. \tag{10}$$

此與 (9) 式相矛盾．故使 (5) 式成立之 $n\ (\leqslant x)$ 的個數必爲 $o(x)$．定理得證．

由此定理可知：對幾乎所有的 n，常有

$$\omega(n)\sim\log\log n \quad 及 \quad \Omega(n)\sim\log\log n.$$

§ 11. 表素數之函數．

定理 1. 有一實數 α 存在，如命

$$\alpha=\alpha_0,\quad 2^{\alpha_0}=\alpha_1,\cdots,\quad 2^{\alpha_n}=\alpha_{n+1},\cdots,$$

則

$$[\alpha_n]$$

常爲一素數．

證： 今用歸納法做一素數列 $\{p_n\}$：取 $p_1=3$，由定理 7.1 可知有一素數 p_{n+1} 適合於

$$2^{p_n}<p_{n+1}<p_{n+1}+1\leqslant 2^{p_n+1}.$$

若 $p_{n+1}+1=2^{p_n+1}$，則 $p_{n+1}=2^{p_n+1}-1$，此非素數（因其有因子 $2^{\frac{1}{2}(p_n+1)}-1$），故

$$2^{p_n}<p_{n+1}<p_{n+1}+1<2^{p_n+1}.$$

以 2 爲底作對數，並定義

$$\log^{(n)}x=\log^{(n-1)}(\log x).$$

作數列

$$u_n=\log^{(n)}p_n,\qquad v_n=\log^{(n)}(p_n+1).$$

則由

$$p_n<\log p_{n+1}<\log\ (p_{n+1}+1)<p_n+1,$$

可知

$$u_n<u_{n+1}<v_{n+1}<v_n,$$

卽 u_n 成一遞增貫數，v_n 成一遞降貫數，故有一實數 α 存在使

$$\lim_{n\to\infty}u_n=\alpha,$$

且

$$u_n<\alpha<v_n.$$

卽得

$$p_n < \alpha_n < p_n + 1,$$

故

$$[\alpha_n] = p_n.$$

習題 1. 證明 並無一個非常數的整係數多項式 $f(x)$，能對任一整數 n，$f(n)$ 常為素數.

習題 2. 命 $P(x_1, x_2, \cdots, x_k)$ 表一整係數多項式. 命

$$f(n) = P(n, 2^n, 3^n, \cdots, k^n).$$

若當 $n \to \infty$ 時，$f(n) \to \infty$，則 $f(n)$ 代表無窮個複合數.

§12. 等差級數中之素數問題.

由 §5 之習題已知形如 $4n-1$ 及 $6n-1$ 之素數之個數無窮. 因之建議次之定理:

若 a, b 互素，則形如 $an+b$ 之素數之個數無窮.

此乃著名之 Dirichlet 定理是也，其證明見第九章. 今將證明若干特例:

可設 $a > 0$, $b > 0$. 若能證明有一形如 $an+b$ $(n > 0)$ 之素數存在，則 Dirichlet 定理卽已證明. 何則? 若有一 n 使

$$an + b = p_1 \,(> b)$$

為素數，又有一 n 使

$$ap_1 n + b = p_2 \,(> p_1)$$

為素數，等等. 則有無窮個形如 $an+b$ 之素數存在.

定理 1. 命 $k > 1$. 形如 $kn+1$ 之素數之個數無窮.

由前所述，如能證明有一如此之素數卽足.

方程式 $x^k = 1$ 之解答為

$$e^{2\pi i a/k}, \qquad a = 0, 1, \cdots, k-1.$$

命

$$F_n(x) = \prod_{(a,n)=1} (x - e^{2\pi i a/n}),$$

此乘積中求積變數 a 過 n 之縮系.

顯然

$$x^k - 1 = \prod_{n|k} F_n(x),$$

此乘積之 n 過 k 之諸因子. 蓋等式左邊之每根必在右邊出現. 反之,右邊之每根又必在左邊出現,且無重複. 命

$$x^k-1=F_k(x)\,G_k(x),$$

此 $G_k(x)$ 乃諸多項式 x^n-1 $(n|k,\ n<k)$ 之最小公倍式,且其第一係數爲 1. 故 $G_k(x)$ 乃一整係數之多項式. 由定理 1.13.2 可知 $F_k(x)$ 亦爲整係數多項式.

若 x 爲非 ± 1 之整數,則

$$F_k(x)\,G_k(x)\neq 0,$$

即 $F_k(x)$ 及 $G_k(x)$ 爲二異於零之整數.

引 1. 若 n 爲 k 之眞因子,則對非 ± 1 之整數 x, 有次之結果:

$$\left(x^n-1,\ \frac{x^k-1}{x^n-1}\right)\Big|\,k.$$

證: 命 $x^n-1=y$, $k=nd$, 則

$$\frac{x^k-1}{x^n-1}=\frac{(y+1)^d-1}{y}=y^{d-1}+\binom{d}{1}y^{d-2}+\cdots+\binom{d}{2}y+d\equiv$$
$$\equiv d \pmod y.$$

故得所云.

引 2. 若 x 爲非 ± 1 之整數, 則 $F_k(x)$ 及 $G_k(x)$ 之公共素因子必爲 k 之因子.

證: 假定素數 p 整除 $(F_k(x), G_k(x))$. 由

$$p\,|\,G_k(x)=\prod_{\substack{n|k\\ n<k}}F_n(x)$$

可知,必有一 n 使

$$p\,|\,F_n(x)\qquad (n|k,\ n<k),$$

故

$$p\,|\,x^n-1.$$

再由 $p\,|\,F_k(x)$, 可知

$$p\,\Big|\,\frac{x^k-1}{x^n-1}.$$

即

$$p \,\Big|\, \left(x^n-1,\ \frac{x^k-1}{x^n-1}\right).$$

由引一卽得所求.

定理 1 之證明: 命 $x = ky$, 則

$$F_k(x)\, G_k(x) = x^k - 1 \equiv -1 \pmod{k}.$$

吾人可選擇 y 使

$$F_k(x) \neq \pm 1,$$

因方程式 $F_k(x) = \pm 1$ 僅有有限個根,故此種選擇必爲可能.

$F_k(x)$ 中至少有一素因子 p, 由引二,此必非 $G_k(x)$ 之因子. 換言之,對任一 k 之眞因子 n,

$$x^n \not\equiv 1 \pmod{p}. \tag{1}$$

但

$$x^k \equiv 1 \pmod{p}.$$

茲往證明 $k|p-1$. 若不然,有二整數 s 及 t 使

$$(k, p-1) = sk + t(p-1).$$

卽對 $n = (k, p-1)$ 有

$$x^n \equiv (x^k)^s\,(x^{p-1})^t \equiv 1 \pmod{p}.$$

此與 (1) 相矛盾. 卽 $p \equiv 1 \pmod{k}$, 卽有一形如 $kn+1$ 之素數存在. 故定理得證.

習題. 有無窮個形如 $8n+5$ 之素數.

提示: 討論 $q = 3^2 \cdot 5^2 \cdot 7^2 \cdots p^2 + 2^2$, 並證明凡 $x^2 + y^2$ 之素因子 p 必 $\equiv 1 \pmod{4}$.

第　六　章

數　論　函　數

§1. 數論函數舉例.

定 義 1. 對任一正整數 n, 有一定數值之函數 $f(n)$ 謂之數論函數.

例如: 貫數 a_n 可視爲數論函數. 具體例子如: $n!$, $\sin n$, $d(n) = \sum_{d|n} 1$, $n = x^2 + y^2$ 之解數 $r(n)$ 等.

定 義 2. 一數論函數如具有次列性質,則謂之積性函數: 若 $(a,b) = 1$, 則

$$f(ab) = f(a)\,f(b). \tag{1}$$

若不論有無 $(a, b) = 1$ 之關係,常有上式,則該數論函數謂之完全積性函數.

由此可知,若 $f(n)$ 爲積性函數, $p_1, \cdots, p_r$ 爲不同的素數,則

$$f(p_1^{a_1} \cdots p_r^{a_r}) = f(p_1^{a_1}) \cdots f(p_r^{a_r}),$$

卽若已知 $f(n)$ 當 n 爲素數乘方時之數值,則 $f(n)$ 已完全决定. 又若 $f(n)$ 是完全積性函數,則

$$f(p_1^{a_1} \cdots p_r^{a_r}) = (f(p_1))^{a_1} \cdots (f(p_r))^{a_r},$$

可知若已知 $f(n)$ 當 n 爲素數時之數值,則 $f(n)$ 已完全决定.

顯然, 二積性函數之積仍爲積性函數. 二完全積性函數之積仍爲完全積性函數.

例 1. 函數

$$\Delta(n) = \begin{cases} 1, & \text{若 } n = 1, \\ 0, & \text{若 } n \neq 1 \end{cases}$$

是一完全積性函數.

例 2. 函數

$$E_\lambda(n) = n^\lambda$$

是一完全積性函數.

例 3. Möbius 函數

$$\mu(n)=\begin{cases}1, & \text{若 } n=1,\\ (-1)^r, & \text{若 } n \text{ 爲 } r \text{ 個不同素數之積},\\ 0, & \text{若 } n \text{ 爲一素數之平方所整除}.\end{cases}$$

極易算出

$$\mu(1)=1,\ \mu(2)=-1,\ \mu(3)=-1,\ \mu(4)=0,\ \mu(5)=-1,\ \mu(6)=1,$$
$$\mu(7)=-1,\ \mu(8)=0,\ \mu(9)=0,\ \mu(10)=1,\ \mu(11)=-1,\cdots$$

此爲一積性函數,但非完全積性函數.

例 4. Euler 函數 $\varphi(n)$,卽不大於 n 之整數而與 n 互素者之個數. 此亦係積性函數,但非完全積性函數.

例 5. 除數函數

$$d(n)=\sum_{d\mid n}1$$

也是一積性函數,但非完全積性函數. 更普遍些,

$$\sigma_\lambda(n)=\sum_{d\mid n}d^\lambda$$

也是一積性函數. 顯然 $\sigma_0(n)=d(n)$.

例 6. von Mangoldt 函數 $\Lambda(n)$:

$$\Lambda(n)=\begin{cases}\log p, & \text{若 } n \text{ 乃素數 } p \text{ 之正乘方},\\ 0, & \text{不然}.\end{cases}$$

卽 $\Lambda(1)=0,\ \ \Lambda(2)=\log 2,\ \ \Lambda(3)=\log 3,\ \ \Lambda(4)=\log 2,\ \ \Lambda(5)=\log 5,$

$\Lambda(6)=0,\ \ \Lambda(7)=\log 7,\ \ \Lambda(8)=\log 2,\ \ \Lambda(9)=\log 3,\ \ \Lambda(10)=0,\cdots.$

此一函數是非積性的.

例 7. 函數

$$\Lambda_1(n)=\begin{cases}\dfrac{1}{m}, & \text{若 } n \text{ 是一素數之 } m(>0) \text{ 次乘方},\\ 0, & \text{若不然}.\end{cases}$$

卽 $\Lambda_1(1)=0,\ \Lambda_1(2)=1,\ \Lambda_1(3)=1,\ \Lambda_1(4)=\frac{1}{2},\ \Lambda_1(5)=1,\ \Lambda_1(6)=0,$

$\Lambda_1(7)=1,\ \Lambda_1(8)=\frac{1}{3},\ \Lambda_1(9)=\frac{1}{2},\ \Lambda_1(10)=0,\cdots$. 此一函數也非積性的.

例 8. 命 p 是一固定素數. 若 $p^{a}\|n$, 定義

$$V_p(n)=p^{-a}.$$

此函數也是完全積性函數. 並不難證明

$$V_p(n+m)\leqslant \max\left(V_p(n),\,V_p(m)\right).$$

例 9. 命 $r(n)$ 表

$$n=x^2+y^2$$

之解數. 以後 (§7) 將證明 $\frac{1}{4}r(n)$ 是一積性函數. 但由於 $r(3)=0$, $r(9)=4$, 可知其非完全積性函數.

§2. 積性函數之性質.

定理 1. 一非恆等於 0 之積性函數 $f(n)$ 在 1 時之值爲 1.

證: 設 $f(a)\neq 0$, 由

$$f(a)=f(a)\,f(1)$$

可知 $f(1)=1$.

定理 2. 若 $g(n)$, $h(n)$ 都是積性函數,則

$$f(n)=\sum_{d|n} g(d)\,h\left(\frac{n}{d}\right)=\sum_{d|n} g\left(\frac{n}{d}\right)h(d) \tag{1}$$

也是積性函數.

證: 後之等式,可由代換 $d'=\frac{n}{d}$ 得之.

假定 $(a,b)=1$, 則

$$f(a\,b)=\sum_{d|ab} g(d)\,h\left(\frac{ab}{d}\right).$$

命 $u=(a,d)$, $v=(b,d)$, 則 $uv=d$, 故

$$\begin{aligned} f(a\,b)&=\sum_{u|a}\sum_{v|b} g(uv)\,h\left(\frac{ab}{uv}\right)=\\ &=\sum_{u|a} g(u)\,h\left(\frac{a}{u}\right)\sum_{v|b} g(v)\,h\left(\frac{b}{v}\right)=\\ &=f(a)\,f(b)\,. \end{aligned}$$

定理 3. 若 $f(n)$ 是一非恆等於零之積性函數,則

$$\sum_{d|n} \mu(d) f(d) = \prod_{p|n} (1-f(p)), \tag{2}$$

此處 p 過 n 之不同的素因子.

證: 於上定理中取 $g(n) = \mu(n) f(n)$, $h(n) = 1$, 可知 (2) 式之左邊是積性的. 其右邊是積性的也一眼可知. 所以僅須證明 $n = 1$ 及 $n = p^l$ 時之情況. 此二種情況極易直接算出.

定理 4. 若 $f(n)$ 是積性的,則

$$f((m, n)) f([m, n]) = f(m) f(n),$$

此處 $[m, n]$ 代表 m, n 之最小公倍數.

證: 命

$$m = p_1^{l_1} \cdots p_s^{l_s}, \qquad l_v \geqslant 0,$$

$$n = p_1^{r_1} \cdots p_s^{r_s}, \qquad r_v \geqslant 0,$$

則

$$f(m) = f(p_1^{l_1}) \cdots f(p_s^{l_s}),$$

$$f(n) = f(p_1^{r_1}) \cdots f(p_s^{r_s}),$$

$$f((m, n)) = f(p_1^{\min(l_1, r_1)}) \cdots f(p_s^{\min(l_s, r_s)}),$$

$$f\left(\frac{m n}{(m, n)}\right) = f(p_1^{\max(l_1, r_1)}) \cdots f(p_s^{\max(l_s, r_s)}).$$

由於

$$f(p^l) f(p^r) = f(p^{\max(l,r)}) f(p^{\min(l,r)}),$$

故得定理.

§ 3. Möbius 反轉公式.

定理 1. 對任一 $n > 0$, 常有

$$\sum_{d|n} \mu(d) = \sum_{d|n} \mu(n/d) = \Delta(n) = \begin{cases} 1, & \text{若 } n = 1, \\ 0, & \text{若 } n \neq 1. \end{cases}$$

此乃定理 2.3 之特例,於其中取 $f(d) = 1$ 即明.

定理 2. 命 $0 < \eta_0 \leqslant \eta_1$. 設 $h(k)$ 是一非恆等於零之完全積性函數.

若對所有適合於 $\eta_0 \leqslant \eta \leqslant \eta_1$ 之 η 常有

$$g(\eta) = \sum_{1 \leqslant k \leqslant \eta_1/\eta} f(k\eta)\, h(k), \tag{1}$$

則對如此之 η 亦常有

$$f(\eta) = \sum_{1 \leqslant k \leqslant \eta_1/\eta} \mu(k)\, g(k\eta)\, h(k); \tag{2}$$

且其逆亦眞實.

證: 由 (1) 可知

$$\sum_{1 \leqslant k \leqslant \eta_1/\eta} \mu(k)\, g(k\eta)\, h(k) = \sum_{1 \leqslant k \leqslant \eta_1/\eta} \mu(k)\, h(k) \sum_{1 \leqslant m \leqslant \eta_1/k\eta} f(mk\eta)\, h(m).$$

命 $mk = r$, 由定理 1 可知

$$\sum_{1 \leqslant k \leqslant \eta_1/\eta} \mu(k)\, g(k\eta)\, h(k) = \sum_{1 \leqslant k \leqslant \eta_1/\eta} \mu(k) \sum_{\substack{1 \leqslant r \leqslant \eta_1/\eta \\ k|r}} f(r\eta)\, h(k)\, h\left(\frac{r}{k}\right) =$$

$$= \sum_{1 \leqslant r \leqslant \eta_1/\eta} f(r\eta)\, h(r) \sum_{\substack{1 \leqslant k \leqslant \eta_1/\eta \\ k|r}} \mu(k) =$$

$$= \sum_{1 \leqslant r \leqslant \eta_1/\eta} f(r\eta)\, h(r) \sum_{k|r} \mu(k) =$$

$$= \sum_{1 \leqslant r \leqslant \eta_1/\eta} f(r\eta)\, h(r)\, \Delta(r) = f(\eta)\, h(1) = f(\eta),$$

此卽 (2) 式.

又設 (2) 式眞實,則

$$\sum_{1 \leqslant k \leqslant \eta_1/\eta} f(k\eta)\, h(k) = \sum_{1 \leqslant k \leqslant \eta_1/\eta} h(k) \sum_{1 \leqslant m \leqslant \eta_1/k\eta} \mu(m)\, g(mk\eta)\, h(m) =$$

$$= \sum_{1 \leqslant k \leqslant \eta_1/\eta} \sum_{\substack{1 \leqslant r \leqslant \eta_1/\eta \\ k|r}} \mu(r/k)\, g(r\eta)\, h(k)\, h(r/k) =$$

$$= \sum_{1 \leqslant r \leqslant \eta_1/\eta} g(r\eta)\, h(r) \sum_{\substack{1 \leqslant k \leqslant \eta_1/\eta \\ k|r}} \mu(r/k) =$$

$$= \sum_{1 \leqslant r \leqslant \eta_1/\eta} g(r\eta)\, h(r)\, \Delta(r) = g(\eta)$$

此卽 (1) 式.

此定理之一推論如次:

定理 3. 命 $\xi_0 \geqslant 1$. 設 $H(k)$ 是一非恆等於零之完全積性函數. 若對所有的適合 $1 \leqslant \xi \leqslant \xi_0$ 之 ξ 常有

$$G(\xi) = \sum_{1 \leqslant k \leqslant \xi} F(\xi/k) H(k), \tag{3}$$

則對此 ξ 也有

$$F(\xi) = \sum_{1 \leqslant k \leqslant \xi} \mu(k) G(\xi/k) H(k); \tag{4}$$

且其逆亦眞.

證: 命 $f(\eta) = F(1/\eta)$ 及 $g(\eta) = G(1/\eta)$. 則由 (3) 及 (4) 有

$$g(\eta) = G(1/\eta) = \sum_{1 \leqslant k \leqslant 1/\eta} F\left(\frac{1}{\eta k}\right) H(k) = \sum_{1 \leqslant k \leqslant 1/\eta} f(\eta k) H(k),$$

$$f(\eta) = F(1/\eta) = \sum_{1 \leqslant k \leqslant 1/\eta} \mu(k) G\left(\frac{1}{\eta k}\right) H(k) = \sum_{1 \leqslant k \leqslant 1/\eta} \mu(k) g(\eta k) H(k).$$

而此乃 (1),(2) 之形式其中 $\eta_1 = 1 \geqslant 1/\xi_0 = \eta_0$ 者.

今舉一例以明其用.

定理 4. 當 $\xi \geqslant 1$ 時,有

$$\left| \sum_{1 \leqslant k \leqslant \xi} \frac{\mu(k)}{k} \right| \leqslant 1. \tag{5}$$

證: 在 (3) 式中取 $F(\xi) = H(k) = 1$, 如此則 $G(\xi) = [\xi]$. 由 (4) 式可知

$$1 = \sum_{1 \leqslant k \leqslant \xi} \mu(k) \left[\frac{\xi}{k}\right]. \tag{6}$$

若 $1 \leqslant \xi < 2$, 則 (5) 式顯然成立. 今設 $\xi \geqslant 2$, 並取 $x = [\xi]$. 則

$$\left| x \sum_{k=1}^{x} \frac{\mu(k)}{k} - 1 \right| = \left| \sum_{k=1}^{x} \mu(k) \left(\frac{x}{k} - \left[\frac{x}{k}\right] \right) \right| =$$

$$= \left| \sum_{k=2}^{x} \mu(k) \left(\frac{x}{k} - \left[\frac{x}{k}\right] \right) \right| \leqslant \sum_{k=2}^{x} 1 = x - 1.$$

故

$$x \left| \sum_{k=1}^{x} \frac{\mu(k)}{k} \right| \leqslant 1 + (x-1) = x,$$

卽得定理.

§4. Möbius 變換.

定理 3.3 之另一推論如下:

定理 1. 命 $h(k)$ 表一非恆等於 0 之完全積性函數,又 n_0 是一正整數. 若對所有 $n \leqslant n_0$, 常有

$$g(n) = \sum_{d|n} f(d)\, h\left(\frac{n}{d}\right), \tag{1}$$

則對此 n 也有

$$f(n) = \sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right) h(d); \tag{2}$$

反之亦然.

證: 若 ξ 是一整數, 則取 $F(\xi) = f(\xi)$, 不然, 則取 $F(\xi) = 0$, $G(\xi)$ 與 $g(\xi)$ 之關係亦然. (1) 及 (2) 式可寫爲

$$G(n) = g(n) = \sum_{d|n} f(d)\, h\left(\frac{n}{d}\right) = \sum_{k|n} f\left(\frac{n}{k}\right) h(k) = \sum_{1 \leqslant k \leqslant n} F\left(\frac{n}{k}\right) h(k)$$

及

$$F(n) = f(n) = \sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right) h(d) = \sum_{d|n} \mu(d)\, G\left(\frac{n}{d}\right) h(d) =$$

$$= \sum_{1 \leqslant d \leqslant n} \mu(d)\, G\left(\frac{n}{d}\right) h(d).$$

又由 $G(\xi)$ 及 $F(\xi)$ 之定義,此二等式亦可寫爲

$$G(\xi) = \sum_{1 \leqslant k \leqslant \xi} F\left(\frac{\xi}{k}\right) h(k),$$

$$F(\xi) = \sum_{1 \leqslant k \leqslant \xi} \mu(k)\, G\left(\frac{\xi}{k}\right) h(k).$$

此處 ξ 適合於 $1 \leqslant \xi \leqslant n_0$. 反之,由此亦可引出 (1) 及 (2) 式,應用定理 3.3 (其中 $\xi_0 = n_0$) 卽得定理.

定義. 若

$$g(n) = \sum_{d|n} f(d) = \sum_{d|n} f\left(\frac{n}{d}\right),$$

則 $g(n)$ 稱爲 $f(n)$ 之 Möbius 變換. 而 $f(n)$ 稱爲 $g(n)$ 之 Möbius 逆變換.

由定理 1 已知

$$f(n)=\sum_{d|n}\mu(d)\,g\left(\frac{n}{d}\right)=\sum_{d|n}\mu\left(\frac{n}{d}\right)g(d).$$

由定理 2.2 可知積性函數之 Möbius 變換及 Möbius 逆變換也是積性函數.

例 1. 由定理 3.1 可知 $\Delta(n)$ 是 $\mu(n)$ 的 Möbius 變換.

例 2. 由定義

$$\sigma_\lambda(n)=\sum_{d|n}d^\lambda.$$

$\sigma_\lambda(n)$ 乃積性函數 $E_\lambda(n)=n^\lambda$ 之 Möbius 變換. 因此 $\sigma_\lambda(n)$ 是積性函數. 由於

$$\sigma_\lambda(p^l)=\sum_{m=0}^{l}p^{m\lambda}=\frac{p^{\lambda(l+1)}-1}{p^\lambda-1}\qquad(\lambda\neq 0),$$

可得出: 若 $n=\prod_\nu p_\nu^{l_\nu}$ 是 n 的標準分解式,則

$$\sigma_\lambda(n)=\prod_\nu\frac{p_\nu^{\lambda(l_\nu+1)}-1}{p_\nu^\lambda-1}.$$

當 $\lambda=0$, 則

$$d(n)=\sigma_0(n)=\prod_\nu(l_\nu+1).$$

此乃吾人所習知者.

例 3. 函數 $E_0(n)=1$ 是 $\Delta(n)$ 之 Möbius 變換.

例 4. 依 $d=(n,a)$ 將正整數 $1,2,\cdots,a,\cdots,n$ 分類. 若 $d=(n,a)$ 則可書 $n=dk$, 而 $1=\left(k,\frac{a}{d}\right)$. 故適合 $1=\left(k,\frac{a}{d}\right)$ 之整數 a 之個數等於 $\varphi\left(\frac{n}{d}\right)$. 即得

$$n=\sum_{d|n}\varphi\left(\frac{n}{d}\right)=\sum_{d|n}\varphi(d).$$

即函數 $E_1(n)=n$ 乃 $\varphi(n)$ 之 Möbius 變換. 由此可以得出第二章 §5 之結果: (i) $\varphi(n)$ 是積性的, (ii) 由 Möbius 之反轉公式可得:

定理 2.

$$\varphi(n)=n\sum_{d|n}\frac{\mu(d)}{d}.$$

例 5. 更廣義些,命 $\varphi_\lambda(n)$ 爲 $E_\lambda(n)$ 之 Möbius 逆變換,故 $\varphi_1(n)=\varphi(n)$. 則 $\varphi_\lambda(n)$ 是一積性函數. 且當 $n=\prod_\nu p_\nu^{l_\nu}$ 時,有

$$\varphi_\lambda(n)=n^\lambda\sum_{d|n}\frac{\mu(d)}{d^\lambda}=n^\lambda\prod_{p|n}\left(1-\frac{1}{p^\lambda}\right).$$

證明留給讀者.

例 6. 以素數 p 爲模,把多項式

$$x^{p^n}-x$$

分解爲不可化多項式之積. 其因子之次數爲 m, 且已知 $m|n$. 反之, 任一 m 次不可化多項式一定是該式之因子. 命 Φ_n 表對模 p, n 次不可化多項式之個數. 則關於多項式之次數有次之等式

$$p^n=\sum_{m|n}m\,\Phi_m\,.$$

卽函數 p^n 乃 $n\Phi_n$ 之 Möbius 變換. 由反轉公式可知

$$n\,\Phi_n=\sum_{m|n}\mu(m)\,p^{\frac{n}{m}}.$$

此又證明了定理 4.9.2.

例 7. 今往求 $\Lambda(n)$ 之 Möbius 變換. 命 $n=p_1^{l_1}\cdots p_r^{l_r}$ 爲 n 之標準分解式, 則

$$\begin{aligned}\sum_{d|n}\Lambda(d)&=\sum_{s_1=0}^{l_1}\cdots\sum_{s_r=0}^{l_r}\Lambda(p_1^{s_1}\cdots p_r^{s_r})=\\&=\sum_{s_1=1}^{l_1}\Lambda(p_1^{s_1})+\cdots+\sum_{s_r=1}^{l_r}\Lambda(p_r^{s_r})=\\&=\sum_{s_1=1}^{l_1}\log p_1+\cdots+\sum_{s_r=1}^{l_r}\log p_r=\\&=l_1\log p_1+\cdots+l_r\log p_r=\\&=\log n\,,\end{aligned}$$

卽 $\log n$ 是 $\Lambda(n)$ 之 Möbius 變換.

例 8. 因爲 $\Lambda(n)$ 是 $\log n$ 之 Möbius 逆變換,故

$$\Lambda(n)=\sum_{d|n}\mu(d)\log n/d=\log n\sum_{d|n}\mu(d)-\sum_{d|n}\mu(d)\log d=$$

$$= \Delta(n)\log n - \sum_{d|n}\mu(d)\log d.$$

由於 $\Delta(n)\log n$ 恆等於零,故 $\Lambda(n)$ 乃 $-\mu(n)\log n$ 之 Möbius 變換.

總括此諸結果可有次表,其中 $g(n)$ 代表 $f(n)$ 之 Möbius 變換:

$f(n)$	$\mu(n)$	$\Delta(n)$	$\varphi_\lambda(n)$	$E_\lambda(n)$	$-\mu(n)\log n$	$\Lambda(n)$
$g(n)$	$\Delta(n)$	$E_0(n)$	$E_\lambda(n)$	$\sigma_\lambda(n)$	$\Lambda(n)$	$\log n$

習題 1. 若 $g(n)$ 及 $g_1(n)$ 各爲 $f(n)$ 及 $f_1(n)$ 之 Möbius **變換, 試證明**

$$\sum_{d|n} g(d)\, f_1\left(\frac{n}{d}\right) = \sum_{d|n} f(d)\, g_1\left(\frac{n}{d}\right).$$

習題 2. 求出 $g(n)g_1(n)$ 之 Möbius 逆變換.

習題 3. $f(n)$ 之 Möbius 變換之 Möbius 變換等於

$$\sum_{d_1|n} f(d_1)\, d\left(\frac{n}{d_1}\right).$$

習題 4. 用證明例 6 之方法. 證明 4.10(1) 式.

§ 5. 除數函數.

定理 1. 常有

$$d(mn) \leqslant d(m)\, d(n).$$

證: 若 p 爲一素數,則

$$d(p^a \cdot p^b) = d(p^{a+b}) = a+b+1 \leqslant (a+1)(b+1) = d(p^a)\, d(p^b).$$

因爲 $d(n)$ 是一積性函數,故得出定理.

定理 2. 對任一 $\varepsilon > 0$, 常有

$$d(n) = O(n^\varepsilon). \tag{1}$$

此 O 號所包含之常數依於 ε.

證: 命 $n = \prod_{p|m} p^a$ 表 n 之標準分解式. 今有

$$p^{a\varepsilon} \geqslant 2^{a\varepsilon} = e^{a\varepsilon\log 2} \geqslant a\,\varepsilon\log 2 \geqslant \frac{1}{2}(a+1)\,\varepsilon\log 2;$$

且若 $p^\varepsilon \geqslant 2$, 則 $p^{a\varepsilon} \geqslant 2^a \geqslant a+1$. 故

$$\frac{d(n)}{n^{\varepsilon}}=\prod_{p|n}\frac{a+1}{p^{a\varepsilon}}=\prod_{\substack{p|n\\p^{\varepsilon}<2}}\frac{a+1}{p^{a\varepsilon}}\prod_{\substack{p|n\\p^{\varepsilon}\geqslant 2}}\frac{a+1}{p^{a\varepsilon}}\leqslant$$

$$\leqslant\prod_{\substack{p|n\\p^{\varepsilon}<2}}\frac{a+1}{\frac{1}{2}(a+1)\,\varepsilon\log 2}\prod_{\substack{p|n\\p^{\varepsilon}\geqslant 2}}\frac{a+1}{a+1}\leqslant\prod_{p^{\varepsilon}<2}\frac{2}{\varepsilon\log 2},$$

此卽定理.

定理 3. 命 q 爲一整數 $\geqslant 0$, $\xi\geqslant 2$, 則

$$\sum_{1\leqslant n\leqslant\xi}(d(n))^{q}=O(\xi(\log\xi)^{2^{q}-1}),\tag{2}$$

$$\sum_{1\leqslant n\leqslant\xi}\frac{(d(n))^{q}}{n}=O((\log\xi)^{2^{q}}).\tag{3}$$

證: 先證明第二式. 於 q 上行歸納法,吾人已知 $q=0$ 時,此式眞實,並設其對 $q-1$ 時也眞實. 則

$$\sum_{1\leqslant n\leqslant\xi}\frac{(d(n))^{q}}{n}=\sum_{1\leqslant n\leqslant\xi}\frac{(d(n))^{q-1}}{n}\sum_{u|n}1=$$

$$=\sum_{1\leqslant u\leqslant\xi}\sum_{\substack{1\leqslant n\leqslant\xi\\u|n}}\frac{(d(n))^{q-1}}{n}.$$

命 $n=uv$, 並用 $d(uv)\leqslant d(u)d(v)$, 可知

$$\sum_{1\leqslant n\leqslant\xi}\frac{(d(n))^{q}}{n}\leqslant\sum_{1\leqslant u\leqslant\xi}\frac{(d(u))^{q-1}}{u}\sum_{1\leqslant v\leqslant\xi/u}\frac{(d(v))^{q-1}}{v}=$$

$$=O((\log\xi)^{2^{q}}).$$

再證 (2) 式: 仍於 q 上行歸納法,

$$\sum_{1\leqslant n\leqslant\xi}(d(n))^{q}=\sum_{1\leqslant n\leqslant\xi}(d(n))^{q-1}\sum_{u|n}1=$$

$$=\sum_{1\leqslant u\leqslant\xi}\sum_{\substack{1\leqslant n\leqslant\xi\\u|n}}(d(n))^{q-1}\leqslant$$

$$\leqslant\sum_{1\leqslant u\leqslant\xi}(d(u))^{q-1}\sum_{1\leqslant v\leqslant\xi/u}(d(v))^{q-1}\leqslant$$

$$\leqslant\xi\sum_{1\leqslant u\leqslant\xi}\frac{(d(u))^{q-1}}{u}O((\log\xi)^{2^{q-1}-1})=$$

$$= O(\xi (\log \xi)^{2^q-1}).$$

此定理能更精密化,僅舉一十分重要之特例來說明此點.

定理 4. 若 $\xi \geqslant 1$, 則

$$\sum_{1 \leqslant n \leqslant \xi} d(n) = \xi \log \xi + (2\gamma - 1)\xi + O(\sqrt{\xi}),$$

此處 γ 是 Euler 常數.

證: 已知

$$\sum_{1 \leqslant n \leqslant \xi} d(n) = \sum_{1 \leqslant n \leqslant \xi} \sum_{u|n} 1 =$$

$$= \sum_{1 \leqslant uv \leqslant \xi} 1 .$$

換言之, $\sum_{1 \leqslant n \leqslant \xi} d(n)$ 乃等腰雙曲線在第一象限中與二坐標軸間之整點數. (整點云者,乃指其二坐標都是整數之點).

從 $(\sqrt{\xi}, \sqrt{\xi})$ 引二垂直於坐標軸之直線,則該圖形被分爲三塊,其中正方形之外之二塊中之整點數相等,卽

$$\sum_{1 \leqslant uv \leqslant \xi} 1 = [\sqrt{\xi}]^2 + 2 \sum_{u=1}^{[\sqrt{\xi}]} \sum_{[\sqrt{\xi}] < v \leqslant \xi/u} 1 =$$

$$= -[\sqrt{\xi}]^2 + 2 \sum_{u=1}^{[\sqrt{\xi}]} \left[\frac{\xi}{u}\right] =$$

$$= -\xi + O(\sqrt{\xi}) + 2 \sum_{u=1}^{\sqrt{\xi}} \frac{\xi}{u} + O(\sqrt{\xi}).$$

因爲

$$\sum_{u=1}^{\sqrt{\xi}} \frac{1}{u} = \frac{1}{2} \log \xi + \gamma + O\left(\frac{1}{\sqrt{\xi}}\right),$$

故可知

$$\sum_{1 \leqslant n \leqslant \xi} d(n) = \xi \log \xi + (2\gamma - 1)\xi + O(\sqrt{\xi}).$$

習題 1. 證明: 當 $\xi \geqslant 2$ 時,

$$\sum_{1 \leqslant n \leqslant \xi} \frac{d(n)}{n} = \frac{1}{2} \log^2 \xi + 2\gamma \log \xi + c + O(\xi^{-\frac{1}{2}} \log \xi).$$

習題 2. 證明. 對任一 ε, 常有

$$\sigma(n)=O(n^{1+\varepsilon}).$$

習題 3. 證明: 當 $\xi\geqslant 2$ 時,

$$\sum_{1\leqslant n\leqslant\xi}\sigma(n)=\frac{1}{12}\pi^2\xi^2+O(\xi\log\xi).$$

$\left(\text{在證明中將用及}\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}\text{, 此式將在習題 8 7.1 中證明.}\right)$

§6. 關於概率之二定理.

定義 1. 若有一正整數組,其中不大於 x 者之個數 $N(x)$ 適合於

$$\lim_{x\to\infty}\frac{N(x)}{x}=\alpha,$$

則此組之數之出現概率名之爲 α.

例如: 奇數出現概率是 $\frac{1}{2}$. 平方數出現概率是零.

在本節中將用及以下之結果

$$\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}=\frac{6}{\pi^2}. \tag{1}$$

其證明在習題 8.7.1 中.

定義 2. 一正整數如不能爲素數之平方所整除,則謂之無平方因子數.

定理 1. 不超過 x 之無平方因子數之個數以 $Q(x)$ 表之,則

$$Q(x)=\frac{6}{\pi^2}x+O(\sqrt{x}). \tag{2}$$

由此可知,無平方因子數之出現概率爲 $\frac{6}{\pi^2}$.

證: 將不大於 x 之正整數依其最大平方因子 q^2 分類,不大於 x 而有 q^2 爲最大平方因子之正整數之個數爲

$$Q\left(\frac{x}{q^2}\right),$$

故可知

$$[x]=\sum_{q=1}^{[\sqrt{x}]}Q\left(\frac{x}{q^2}\right).$$

命 $x=y^2$, 則

$$[y^2] = \sum_{q=1}^{[y]} Q\left(\left(\frac{y}{q}\right)^2\right).$$

由定理 3.3 可知

$$Q(y^2) = \sum_{1 \leqslant k \leqslant y} \mu(k)\left[\frac{y^2}{k^2}\right] =$$

$$= y^2 \sum_{1 \leqslant k \leqslant y} \frac{\mu(k)}{k^2} + \sum_{1 \leqslant k \leqslant y} O(1) =$$

$$= \frac{6}{\pi^2} y^2 + y^2\ O\left(\sum_{k > y} \frac{1}{k^2}\right) + O(y) =$$

$$= \frac{6}{\pi^2} y^2 + O(y),$$

此即所欲證．（證明時用了（5.8.8）式．）

定理 1 亦可改述爲:

定理 2. 若 $x \geqslant 1$，則

$$\sum_{n \leqslant x} |\mu(n)| = \frac{6}{\pi^2} x + O(\sqrt{x}). \tag{3}$$

定理 3. 適合於

$$1 \leqslant x \leqslant y \leqslant n \tag{4}$$

之整數對 x, y 之對數等於

$$\frac{1}{2} n(n+1),$$

其中 $(x, y) = 1$ 之整數對之數目記之爲 $\Phi(n)$． 今往證明

$$\lim_{n \to \infty} \frac{\Phi(n)}{\frac{1}{2} n(n+1)} = \frac{6}{\pi^2}.$$

也可以說成互素整數對出現的概率是 $\frac{6}{\pi^2}$.

今將證明一更精密的定理:

定理 4.

$$\Phi(n) = \sum_{m \leqslant n} \varphi(m) = \frac{3n^2}{\pi^2} + O(n \log n)$$

證:

$$\Phi(n) = \sum_{m=1}^{n} m \sum_{d \mid m} \frac{\mu(d)}{d} = \sum_{dd' \leqslant n} d'\, \mu(d) =$$

$$= \sum_{d=1}^{n} \mu(d) \sum_{d'=1}^{[n/d]} d' = \frac{1}{2} \sum_{d=1}^{n} \mu(d) \left(\left[\frac{n}{d} \right]^2 + \left[\frac{n}{d} \right] \right) =$$

$$= \frac{1}{2} \sum_{d=1}^{n} \mu(d) \left(\frac{n^2}{d^2} + O\left(\frac{n}{d} \right) \right) =$$

$$= \frac{1}{2} n^2 \sum_{d=1}^{n} \frac{\mu(d)}{d^2} + O\left(n \sum_{d=1}^{n} \frac{1}{d} \right) =$$

$$= \frac{1}{2} n^2 \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + O\left(n^2 \sum_{n+1}^{\infty} \frac{1}{d^2} \right) + O(n \log n) =$$

$$= \frac{3n^2}{\pi^2} + O(n) + O(n \log n) =$$

$$= \frac{3n^2}{\pi^2} + O(n \log n) .$$

明所欲證.

§7. 表整數爲二平方之和.

先引進一數論函數

$$\chi(n) = \begin{cases} 0 & 若 \ 2 \mid n, \\ (-1)^{\frac{1}{2}(n-1)} & 若 \ 2 \nmid n. \end{cases}$$

易證此函數是積性的. 此函數之 Möbius 變換以

$$\delta(n) = \sum_{d \mid n} \chi(d)$$

表之,所以 $\delta(n)$ 也是積性的. 若命 $n = \prod_{p \mid n} p^l$ 表 n 之標準分解式,則

$$\delta(n) = \prod_{p \mid n} (1 + \chi(p) + \chi(p^2) + \cdots + \chi(p^l)) .$$

用函數 $\chi(n)$ 可以將定理 3.5.1 之結果重述如下:

定理 1. 同餘式

$$x^2 \equiv -1 \qquad (\text{mod } n)$$

之解數 $V(n)$ 等於

$$V(n) = \begin{cases} 0, & 若 \ 4 \mid n; \\ \prod_{p \mid n} (1 + \chi(p)), & 若 \ 4 \nmid n, 此處 \ p \ 經過 \ n \ 的所有不同的素因子. \end{cases}$$

此定理不難由定理 3.5.1 及定理 2.8.1 推得之.

本節之主要目的在證明:

定理 2. 命 $r(n)$ 表方程

$$x^2 + y^2 = n$$

之整數解 x, y 之組數,則

$$r(n) = 4\delta(n).$$

在證明此定理時,需幾條預備定理:

定理 3. 常有恆等式

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 + y_1y_2)^2 + (x_1y_2 - y_1x_2)^2.$$

此式極易直接乘出,不再證明.

習題 1. 試證恆等式:

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = \\ = (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 + \\ + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2.\end{aligned}$$

習題 2. 試證恆等式:

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2) \times \\ \times (y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 + y_6^2 + y_7^2 + y_8^2) = \\ = (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 + x_5y_5 + x_6y_6 + x_7y_7 + x_8y_8)^2 + \\ + (x_1y_2 - x_2y_1 - x_3y_4 + x_4y_3 - x_5y_6 + x_6y_5 - x_7y_8 + x_8y_7)^2 + \\ + (x_1y_3 + x_2y_4 - x_3y_1 - x_4y_2 + x_5y_7 - x_6y_8 - x_7y_5 + x_8y_6)^2 + \\ + (x_1y_4 - x_2y_3 + x_3y_2 - x_4y_1 - x_5y_8 - x_6y_7 + x_7y_6 + x_8y_5)^2 + \\ + (x_1y_5 + x_2y_6 - x_3y_7 + x_4y_8 - x_5y_1 - x_6y_2 + x_7y_3 - x_8y_4)^2 + \\ + (x_1y_6 - x_2y_5 + x_3y_8 + x_4y_7 + x_5y_2 - x_6y_1 - x_7y_4 - x_8y_3)^2 + \\ + (x_1y_7 + x_2y_8 + x_3y_5 - x_4y_6 - x_5y_3 + x_6y_4 - x_7y_1 - x_8y_2)^2 + \\ + (x_1y_8 - x_2y_7 - x_3y_6 - x_4y_5 + x_5y_4 + x_6y_3 + x_7y_2 - x_8y_1)^2.\end{aligned}$$

定理 4. 命 $n > 1$, 對應於

$$l^2 \equiv -1 \pmod{n} \tag{1}$$

之一解,有一對且唯有一對整數 x, y 使

$$x^2+y^2=n,\quad x>0,\quad y>0,\quad (x,y)=1,\quad y\equiv lx \pmod n. \tag{2}$$

證: 顯然,若 (2) 式有一解,則 (1) 式有一解.

(1) 式有解之必要且充分之條件爲 n 可表成

$$n=2^a p_1^{l_1}\cdots p_s^{l_s},\qquad a=0 \text{ 或 } 1,$$

而 $p_i(i=1,2,\cdots,s)$ 則是 $\equiv 1 \pmod 4$ 之素數. 今利用歸納法來證明本定理.

1) $n=p^\lambda$ 之情況: 若 $\lambda=1$, 則由 $l^2+1\equiv 0 \pmod p$, 可知當 $(x,p)=1$ 時有

$$x^2l^2+x^2\equiv 0 \pmod p.$$

今決定 y 及 x 使

$$x^2l^2\equiv y^2 \pmod p,$$

且 $x^2<p, y^2<p$. 於差數 $xl-y$ 中,命 x, y 分別取 $0,1,\cdots,[\sqrt p]$,共 $[\sqrt p]+1$ 個值,則得 $([\sqrt p]+1)^2>p$ 個差數, 故其必有兩個關於 p 爲同餘. 設

$$x_1 l-y_1\equiv x_2 l-y_2 \pmod p,$$

卽

$$(x_1-x_2)l\equiv y_1-y_2 \pmod p,$$

不妨假定 $x_1-x_2>0$, 則

$$x_1-x_2<\sqrt p,\qquad |y_1-y_2|<\sqrt p$$

卽爲所欲求之 x, y. 對此 x, y 有

$$x^2+y^2=tp,$$

易見 $t=1$, $(x,y)=1$.

同餘式

$$y\equiv mx \pmod p$$

有解,由是 $x^2(1+m^2)\equiv 0 \pmod p$, 故必 $m\equiv \pm l$, 若 $m=l$, 則 (x,y) 卽爲所求,若 $m=-l$, 則 (y,x) 卽爲所求.

今設 $p\neq 2$, 而定理對 p^λ 成立. 設 $(-l)^2\equiv -1 \pmod{p^{\lambda+1}}$, 故有 u, v 使

$$p^\lambda=u^2+v^2,\quad u>0,\quad v>0,\quad (u,v)=1,\quad v\equiv -lu \pmod{p^\lambda}.$$

則當 $n=p^{\lambda+1}$ 時,

$$p^{\lambda+1} = (xu + yv)^2 + (xv - yu)^2 = X^2 + Y^2 \qquad (X > 0,\ Y > 0).$$

(i) $(X, Y) = 1$，蓋若不然，則必 $p \mid (X, Y)$，但

$$X \equiv xu + yv \equiv xu - l^2xu \equiv xu\,(1-l^2) \not\equiv 0 \qquad (\bmod p),$$

此不可能.

(ii) 因爲 $(X, p) = 1$，故同餘式

$$Xm \equiv Y \qquad (\bmod p^{\lambda+1})$$

有解。 由是得

$$X^2 + X^2m^2 \equiv 0 \qquad (\bmod p^{\lambda+1}),$$

即

$$1 + m^2 \equiv 0 \qquad (\bmod p^{\lambda+1}).$$

由定理 2.9.3，此同餘式僅有二解，故

$$m = \pm l.$$

依照 $\lambda = 1$ 之情形進行討論，即明所欲.

2) 設 $n = ab$，$a > 1$，$b > 1$，$(a, b) = 1$. 又設

$$l^2 \equiv -1 \qquad (\bmod n),$$

$$u^2 + v^2 = a, \quad u > 0, \quad v > 0, \quad (u, v) = 1, \quad v \equiv lu \qquad (\bmod a),$$

$$x^2 + y^2 = b, \quad x > 0, \quad y > 0, \quad (x, y) = 1, \quad y \equiv lx \qquad (\bmod b).$$

由定理 3 得

$$n = ab = (xv + yu)^2 + (xu - yv)^2 = X^2 + Y^2.$$

(若 $xu - yv > 0$，則命 $xu - yv = Y$，否則，命 $xu - yv = -Y$.)

今證明：

(i) $(X, Y) = 1$. 設 $p > 1$，$p \mid (X, Y)$，則

$$xv + yu = ps,$$

$$xu - yv = pt,$$

即得

$$x\,(u^2 + v^2) = p\,(sv + tu),$$

$$y\,(u^2 + v^2) = p\,(su - tv).$$

因 $(x, y) = 1$，故必 $p \mid (u^2 + v^2)$，即 $p \mid a$. 同理，$p \mid b$. 此與 $(a, b) = 1$ 之假設不合.

(ii) $X\equiv lY \pmod n$. 由假設

$$xv+yu\equiv lxu-lyv\equiv l(xu-yv) \pmod a,$$
$$xv+yu\equiv -lyv+lxu\equiv l(xu-yv) \pmod b.$$

因爲 $(a, b)=1$, 故

$$X\equiv lY \pmod n.$$

3) 唯一性. 設有兩組 (X, Y), (X', Y') 同時適合所設條件,則

$$n^2=(XX'+YY')^2+(XY'-YX')^2.$$

但

$$XX'+YY'\equiv XX'(1+l^2)\equiv 0 \pmod n,$$

故必

$$XX'+YY'=n, \qquad XY'-YX'=0.$$

由 $XY'-YX'=0$, 有 $\frac{X}{X'}=\frac{Y}{Y'}=c$, $X^2+Y^2=c^2(X'^2+Y'^2)$, 故 $c=\pm 1$. 又由 $X>0$, $X'>0$, 知

$$c=1.$$

吾人之定理卽已完全證明.

定理 2 之證明:

由定理 1 及定理 4 可知

$$x^2+y^2=n, \qquad (x, y)=1$$

之解數等於

$$4V(n).$$

今將

$$x^2+y^2=n$$

之解數依 $(x, y)=d$ 分組; $(x, y)=d$ 之解數之等於

$$\left(\frac{x}{d}\right)^2+\left(\frac{y}{d}\right)^2=\frac{n}{d^2},$$

之解數之個數, 卽 $4V\left(\frac{n}{d^2}\right)$. 故得

$$r(n)=4\sum_{d^2|n}V\left(\frac{n}{d^2}\right)=4\sum_{d|n}V\left(\frac{n}{d}\right)\lambda(d),$$

此處 $\lambda(d)=1$ 或 0 視 d 爲平方數與否而定. 因爲 $V(n)$ 及 $\lambda(n)$ 都是積性

的，故 $\frac{r(n)}{4}$ 是積性的.

因 $\delta(n)$ 也是積性的，故若能證明 $n = p^l$ 時，

$$\frac{r(n)}{4} = \delta(n),$$

則定理已明.

若 $2|m$,

$$\frac{r(p^m)}{4} = V(p^m) + V(p^{m-2}) + \cdots + V(p^2) + V(1) =$$

$$= \begin{cases} 0 + \cdots + 0 + 1 = 1, & \text{若 } p = 2, \\ 0 + \cdots + 0 + 1 = 1, & \text{若 } p \equiv 3 \pmod 4, \\ 2 + \cdots + 2 + 1 = & \\ \quad = \frac{m}{2}\cdot 2 + 1 = m + 1, & \text{若 } p \equiv 1 \pmod 4, \end{cases}$$

又若 $2 \nmid m$，則

$$\frac{r(p^m)}{4} = V(p^m) + \cdots + V(p) =$$

$$= \begin{cases} 1, & \text{若 } p = 2, \\ 0, & \text{若 } p \equiv 3 \pmod 4, \\ m + 1, & \text{若 } p \equiv 1 \pmod 4. \end{cases}$$

另一方面

$$\delta(p^m) = 1 + \chi(p) + \cdots + \chi(p^m) =$$

$$= \begin{cases} 1 + 0 + 0 + \cdots + 0 = 1, & \text{若 } p = 2, \\ 1 - 1 + \cdots + 1 = 1, & \text{若 } p \equiv 3 \pmod 4,\ 2 \mid m, \\ 1 - 1 + \cdots - 1 = 0, & \text{若 } p \equiv 3 \pmod 4,\ 2 \nmid m, \\ 1 + 1 + \cdots + 1 = m + 1, & \text{若 } p \equiv 1 \pmod 4. \end{cases}$$

故得定理.

定理 5. 把一整數 n 分為兩個平方和之方法數之四分之一等於 n 之因子之 $\equiv 1 \pmod 4$ 者之個數減去 n 之因子之 $\equiv 3 \pmod 4$ 者之個數.

定理 6. 對任一 $\varepsilon > 0$，常有

$$r(n) = O(n^{\varepsilon}).$$

證: 因爲 $r(n) \leqslant 4d(n)$, 故得定理 (由定理 5.2).

§8. 分部求和法及分部積分法.

定理 1 (Abel). 命 $a \leqslant b$, n 是一變數, 在 $a \leqslant n \leqslant b$ 中變化, γ_n 及 ε_n 是複數. 命

$$s_n = \sum_{a \leqslant m \leqslant n} \gamma_m,$$

則

$$\left|\sum_{n=a}^{b} \gamma_n \varepsilon_n\right| \leqslant \max_{a \leqslant n \leqslant b} |s_n| \left(\sum_{a \leqslant m \leqslant b-1} |\varepsilon_m - \varepsilon_{m+1}| + |\varepsilon_b|\right). \tag{1}$$

證: 命 $s_{a-1} = 0$, 則

$$\sum_{n=a}^{b} \gamma_n \varepsilon_n = \sum_{n=a}^{b} (s_n - s_{n-1}) \varepsilon_n =$$

$$= \sum_{n=a}^{b} s_n \varepsilon_n - \sum_{n=a}^{b-1} s_n \varepsilon_{n+1} =$$

$$= \sum_{n=a}^{b-1} s_n (\varepsilon_n - \varepsilon_{n+1}) + s_b \varepsilon_b,$$

故

$$\left|\sum_{n=a}^{b} \gamma_n \varepsilon_n\right| \leqslant \sum_{n=a}^{b-1} |s_n|\ |\varepsilon_n - \varepsilon_{n+1}| + |s_b|\ |\varepsilon_b| \leqslant$$

$$\leqslant \max_{a \leqslant n \leqslant b} |s_n| \left(\sum_{a \leqslant n \leqslant b-1} |\varepsilon_n - \varepsilon_{n+1}| + |\varepsilon_b|\right).$$

定理 2. 在上定理中,如 ε_n 是正的遞減的實數,則結論可改爲

$$\left|\sum_{n=a}^{b} \gamma_n \varepsilon_n\right| \leqslant \max_{a \leqslant n \leqslant b} |s_n| \varepsilon_a. \tag{2}$$

今舉其一應用如次:

定理 3. 若 $s > 0$, 則

$$\left|\sum_{n \geqslant a} \frac{\chi(n)}{n^s}\right| \leqslant \frac{1}{a^s},$$

故當 $s > 0$ 時級數

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

收斂.

證: 已知

$$\chi(a)+\chi(a+1)+\chi(a+2)+\chi(a+3)=0,$$

故可證明

$$\left|\sum_{a\leqslant m\leqslant b}\chi(m)\right|\leqslant 1.$$

由定理 2 可知

$$\left|\sum_{n=a}^{b}\frac{\chi(n)}{n^s}\right|\leqslant\frac{1}{a^s}.$$

其右邊與 b 無關,故得定理.

附記: 在下節中還將用到

$$\sum_{n=1}^{\infty}\frac{\chi(n)}{n}=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\cdots=\frac{\pi}{4},$$

此可用普通微積分 $\tan^{-1}x$ 之展開式得之.

與定理 1, 2 相仿,有次之定理:

定理 4. 命 $\xi\leqslant\eta$, 變數 x 在 $\xi\leqslant x\leqslant\eta$ 中變化. 設 $f(x)$ 及 $g(x)$ 在此區間中連續,並設 $g(x)$ 可微分. 命

$$f_1(x)=\int_\xi^x f(t)\,dt.$$

則

$$\left|\int_\xi^\eta f(x)\,g(x)\,dx\right|\leqslant\max_{\xi\leqslant x\leqslant\eta}|f_1(x)|\left(\int_\xi^\eta|g'(x)|\,dx+|g(\eta)|\right).$$

又若 $g'(x)\leqslant 0$, $g(x)>0$, 則

$$\left|\int_\xi^\eta f(x)\,g(x)\,dx\right|\leqslant g(\xi)\max_{\xi\leqslant x\leqslant\eta}|f_1(x)|.$$

證: 由分部積分法可知

$$\int_\xi^\eta f(x)\,g(x)\,dx=\int_\xi^\eta g(x)\,d\,f_1(x)=$$

$$=g(\eta)\,f_1(\eta)-\int_\xi^\eta f_1(x)\,g'(x)\,dx,$$

故

$$\left|\int_\xi^\eta f(x)\,g(x)\,dx\right| \leqslant \max_{\xi\leqslant x\leqslant\eta} |f_1(x)|\left(|g(\eta)| + \int_\xi^\eta |g'(x)|\,dx\right).$$

證明之其他部分十分顯然.

例. 設 $a>0$,

$$\left|\int_a^\infty \cos x^2\,dx\right| = \left|\int_{a^2}^\infty \frac{\cos y\,dy}{2y^{1/2}}\right| \leqslant \frac{1}{2a}\max_{a^2\leqslant\eta}\left|\int_{a^2}^\eta \cos y\,dy\right| \leqslant \frac{\pi}{a}.$$

§9. 圓內整點問題.

定理 1.

$$\sum_{1\leqslant n\leqslant x} r(n) = \pi x + O(\sqrt{x}).$$

證: 由定理 7.2 可知

$$\sum_{1\leqslant n\leqslant x} r(n) = 4\sum_{1\leqslant n\leqslant x}\sum_{d|n}\chi(d) =$$

$$= 4\sum_{1\leqslant d\leqslant x}\chi(d)\sum_{\substack{1\leqslant n\leqslant x\\ d|n}} 1 =$$

$$= 4\sum_{1\leqslant d\leqslant x}\chi(d)\left[\frac{x}{d}\right].$$

將此和分爲兩部,由定理 8.3

$$\sum\nolimits_1 = 4\sum_{1\leqslant d\leqslant\sqrt{x}}\chi(d)\left[\frac{x}{d}\right] =$$

$$= 4x\sum_{1\leqslant d\leqslant\sqrt{x}}\frac{\chi(d)}{d} + O(\sqrt{x}) =$$

$$= 4x\sum_{d=1}^\infty\frac{\chi(d)}{d} + O(\sqrt{x}) =$$

$$= \pi x + O(\sqrt{x});$$

其他一部爲

$$\sum\nolimits_2 = 4\sum_{\sqrt{x}<d\leqslant x}\chi(d)\left[\frac{x}{d}\right],$$

由定理 8.2 可知

$$\sum\nolimits_2 = O(\sqrt{x}).$$

總之,得出本定理.

另一證明如下,顯然 $\sum_{1\leqslant n\leqslant x} r(n)$ 是適合

$$u^2+v^2\leqslant x$$

之整數對 u, v 之對數. 換言之,卽爲以 $\sqrt{x}$ 爲半徑以原點爲中心所作圓中之整點的數目. 此圓的面積爲 πx.

在平面上,過整點作與 x 軸及 y 軸平行之直線, 此諸直線將平面分爲方格子. 一圓內整點 (u, v) 對應一方格, 其四頂點爲 (u, v), $(u+1, v)$, $(u, v+1)$, $(u+1, v+1)$. 如此所得之諸方格必在圓

$$u^2+v^2=(\sqrt{x}+\sqrt{2})^2$$

之中,但又包有圓

$$u^2+v^2=(\sqrt{x}-\sqrt{2})^2.$$

故

$$\pi(\sqrt{x}-\sqrt{2})^2\leqslant\sum_{n\leqslant x} r(n)\leqslant\pi(\sqrt{x}+\sqrt{2})^2,$$

卽得定理.

由此證明還偶然地證明了

$$1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\cdots=\frac{\pi}{4}.$$

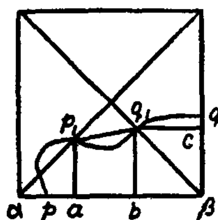
關於更一般的閉曲線內部的整點個數的問題, 捷克數學家 M. V. Jarnik 有次之定理:

定理 2. 命 l 表示一有長的簡單閉曲線的長度,而以 A 表示曲線所範圍區域的面積, N 爲曲線內部所含整點的個數,則若 $l\geqslant 1$, 必有

$$|A-N|<l.$$

證 (Steinhaus): 先證明下面二個簡單的引理:

引 1. 在邊長爲 1 的正方形中,任作一連續曲線 C, C 的兩個端點在正方形的周界上,若 C 與正方形的二對角線相交,則曲線 C 的長 l 必不小於 1.



證: 若 C 的二端點在正方形的一對對邊上, 則顯然 $l\geqslant 1$.

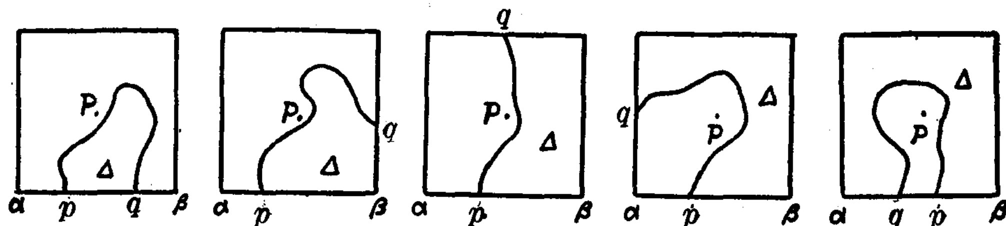
若 C 的端點在正方形的二相隣邊上,如左圖,易見

$$l \geqslant \overline{a p_1} + \overline{p_1 q_1} + \overline{q_1 c} \geqslant \overline{\alpha a} + \overline{a b} + \overline{b \beta} = \overline{\alpha\beta} = 1.$$

至於 C 的二個端點在同一邊上的情形,可用同法證之.

引 2. 在邊長爲 1 的正方形中,任作一不通過正方形中心的連續曲線 C, C 的兩端點在正方形的周界上. 曲線 C 將正方形分爲二部分,命 Δ 爲其中不包含正方形中心的一部分,則 Δ 的面積必小於 C 的長度.

證: 今分別考慮以下各種情形:



命 p, q 表示曲線 C 的端點, P 爲正方形之中心, A, l 各表示Δ的面積及曲線 C 的長度. 則在前二種情形中, 易見從 C 上任何一點到直線 $\alpha\beta$ 的距離必不能大於 l, 故 Δ 完全落在一個邊長爲 1 與 l 的矩形中,因此得到 $A < l$. 在後三種情形中,由引 1 可知 $l \geqslant 1$, 所以有 $A < 1 \leqslant l$. 故引理證畢.

定理的證明: 以 I 表示曲線所範圍的區域,在平面上作網,以直線

$$x = m + \frac{1}{2}, \quad y = n + \frac{1}{2} \qquad (m, n = 0, \pm 1, \pm 2, \cdots)$$

爲經緯,網眼爲邊長爲 1 的正方形. 以 $Q_1, Q_2, \cdots, Q_k$ 表示所有這些小正方形之含有 I 的一部分周界者,而以 C_i 表示有長曲線之在 Q_i 中的部分,以 $\mathfrak{Q}_i$ 表示 Q_i 與 I 的共通部分,而定義

$$N_i = \begin{cases} 1, & \text{若 } \mathfrak{Q}_i \text{ 中有整點}, \\ 0, & \text{若 } \mathfrak{Q}_i \text{ 中無整點}. \end{cases}$$

又以 A_i 表示 $\mathfrak{Q}_i$ 的面積, l_i 表示 C_i 的長度,於是若能證明

$$|A_i - N_i| < l_i,$$

便得定理.

首先我們考慮整個 I 都在某一 Q 中的情形,因爲 $l \geqslant 1$, 故易見定理成立. 因此我們可以不失普遍性地假定 I 並不整個地處在某一 Q 中,此時 C_i 爲若干

段曲線之和，而這些曲線段又將 Q_i 分爲若干個部分 $D_i^{(\nu)}$.

若整點不在任何 $D_i^{(\nu)}$ 中，亦卽當整點在 C_i 上時，有 $N_i=0$, $0<A_i<1$, 而 $l_i\geqslant 1$. 故得所欲證.

若整點在某一 $D_i^{(\nu)}$ 中，以 $A_i^{(\nu)}$ 表示 $D_i^{(\nu)}$ 的面積，若 $D_i^{(\nu)}$ 不在 I 中，此時 $N_i=0$, $A_i\leqslant 1-A_i^{(\nu)}$; 若 $D_i^{(\nu)}$ 在 I 中，則 $N_i=1$, 而 $1-A_i\leqslant 1-A_i^{(\nu)}$, 而由引 2 卽得

$$1-A_i^{(\nu)}<l_i,$$

於是得到定理.

顯然定理 2 也立刻可以導出定理 1.

習題 1. 求出以原點爲中心之橢圓中整點個數之漸近公式.

習題 2. 證明球

$$u^2+v^2+w^2\leqslant x$$

內整點數 $=\frac{4}{3}\pi x^{\frac{3}{2}}+O(x)$.

習題 3. 試推廣上題到 n 度空間之球.

習題 4. 求出

$$\sum_{1\leqslant n\leqslant x} r^2(n)$$

之無窮大之階.

習題 5. 圓內

$$u^2+v^2\leqslant x$$

之兩坐標互素之整點數 $=\frac{6}{\pi}x+O(\sqrt{x}\ \log x)$.

§ 10. Farey 貫及其應用. Farey 貫乃百餘年前之發現，但在近代數論中方顯出其重要性.

定義 1. n 級 Farey 貫者，乃指 0 與 1 之間之諸既約分數，其分母 $\leqslant n$ 者. 其次序依其大小排列，換言之，卽依大小排列之形如

$$\frac{a}{b},\quad (a,b)=1,\qquad 0\leqslant a\leqslant b\leqslant n$$

之諸分數.

n 級 Farey 貫用 $\mathfrak{F}_n$ 表之.

例如：$\mathfrak{F}_7$ 爲

$$\frac{0}{1},\frac{1}{7},\frac{1}{6},\frac{1}{5},\frac{1}{4},\frac{2}{7},\frac{1}{3},\frac{2}{5},\frac{3}{7},\frac{1}{2},$$

$$\frac{4}{7},\frac{3}{5},\frac{2}{3},\frac{5}{7},\frac{3}{4},\frac{4}{5},\frac{5}{6},\frac{6}{7},\frac{1}{1}.$$

$\mathfrak{F}_n$ 中共有 $1+\sum_{m=1}^{n}\varphi(m)$ 個數．此諸數將區間 $0\leqslant x\leqslant 1$ 分爲 $\sum_{m=1}^{n}\varphi(m)$ 份，顯然 $\mathfrak{F}_{n+1}$ 乃由 $\mathfrak{F}_n$ 添加 $\varphi(n+1)$ 個數

$$\frac{a}{n+1},\quad (a,n+1)=1,\qquad 0<a\leqslant n$$

而得者．

定理 1. 命 ξ 表一無理數，$0<\xi<1$．取 n 級 Farey 貫，並設 $\frac{a_m}{b_m}$，$\frac{a'_m}{b'_m}$ 是二鄰項，且適合於

$$\frac{a_m}{b_m}<\xi<\frac{a'_m}{b'_m},$$

則 (i) $\frac{a_m}{b_m}$ 是 n 之遞增函數，$\frac{a'_m}{b'_m}$ 是 n 之遞減函數，且

$$\lim_{n\to\infty}\frac{a_m}{b_m}=\xi=\lim_{n\to\infty}\frac{a'_m}{b'_m};$$

(ii) b_m 及 b'_m 是 n 之遞增函數，且隨 n 趨向無窮．

證： 注意每一有理數皆必爲某一級 Farey 貫中之一數．則由 Farey 貫之定義，定理立可得出．

定理 2. 命 $\frac{a}{b}$，$\frac{a'}{b'}$ 爲 $\mathfrak{F}_n$ 中相鄰之二數．則

$$b+b'\geqslant n+1.$$

若 $\frac{a}{b}<\frac{a'}{b'}$，則

$$ba'-ab'=1.$$

證： 因 $(a,b)=1$，故有整數 x,y，使

$$bx-ay=1,\qquad n-b<y\leqslant n. \tag{1}$$

由此立得

$$y>0,\ (x,y)=1,\ \frac{x}{y}=\frac{a}{b}+\frac{1}{by}>\frac{a}{b}.$$

今祇須證明

$$\frac{x}{y}=\frac{a'}{b'}.$$

因若能證明此式，則 $x=a'$, $y=b'$, $ba'-ab'=1$, 且 $b+b'>n$ 矣. 設此不眞確,卽 $\frac{x}{y}\neq\frac{a'}{b'}$,則

$$\frac{a}{b}<\frac{a'}{b'}<\frac{x}{y}.$$

由此立得

$$\frac{x}{y}-\frac{a}{b}=\frac{x}{y}-\frac{a'}{b'}+\frac{a'}{b'}-\frac{a}{b}\geqslant\frac{1}{b'y}+\frac{1}{b'b}=\frac{b+y}{ybb'}>\frac{n}{ybb'}\geqslant\frac{1}{by}.$$

但由 (1) 已知

$$\frac{x}{y}-\frac{a}{b}=\frac{1}{by},$$

此不能兩立,故得定理.

定理 3. 設 $\frac{a}{b}<\frac{a''}{b''}<\frac{a'}{b'}$ 爲三鄰項,則

$$\frac{a''}{b''}=\frac{a+a'}{b+b'}.$$

證: 由定理 2, 已知

$$a''b-b''a=1,$$

$$a'b''-b'a''=1,$$

相減,立得

$$a''(b+b')-b''(a+a')=0.$$

此卽證明定理.

定義 2. 若 $\frac{a}{b}$ 及 $\frac{a'}{b'}$ 爲二鄰項,則

$$\frac{a+a'}{b+b'}$$

名爲此二項之中項.

定理 4. 中項在該二項之間,與 $\frac{a}{b}$ 及 $\frac{a'}{b'}$ 之距離各爲

$$\frac{1}{b(b+b')},\quad\frac{1}{b'(b+b')}.$$

證: 可設 $\frac{a}{b}<\frac{a'}{b'}$. 則

$$\frac{a'}{b'}-\frac{a+a'}{b+b'}=\frac{ba'-ab'}{b'(b+b')}=\frac{1}{b'(b+b')}>0,$$

$$\frac{a+a'}{b+b'}-\frac{a}{b}=\frac{a'b-ab'}{b(b+b')}=\frac{1}{b(b'+b)}>0.$$

定理 5. 命 ξ 爲一實數,則在 $\mathfrak{F}_n$ 中必有一數 $\frac{a}{b}$,使

$$\left|\xi-\frac{a}{b}\right|<\frac{1}{bn},\qquad 0<b\leqslant n.$$

證: 可設 $0<\xi<1$, 於 $(0, 1)$ 間置 $\mathfrak{F}_n$ 及其諸中項,而將 $(0, 1)$ 分爲若干分隔間. ξ 必在此諸分隔間之一內. 此分隔間一端爲 $\mathfrak{F}_n$ 中之一數 $\frac{a}{b}$, 他端爲一中項 $\frac{a+a'}{b+b'}$. 故

$$\left|\xi-\frac{a}{b}\right|\leqslant\left|\frac{a+a'}{b+b'}-\frac{a}{b}\right|=\frac{1}{b(b+b')}\leqslant\frac{1}{b(n+1)}<\frac{1}{bn}.$$

故得定理. 由此定理立刻可以得出

定理 6. 任與二實數 $\xi, \eta\geqslant 1$, 必有有理數 $\frac{a}{b}$,使

$$\left|\xi-\frac{a}{b}\right|<\frac{1}{b\eta},\qquad 0<b\leqslant\eta.$$

定理 7. 任與一實數 ξ, 吾人有有理數 $\frac{a}{b}$,使

$$\left|\xi-\frac{a}{b}\right|<\frac{1}{b^2}. \tag{2}$$

若 ξ 爲無理數,則有無數個 $\frac{a}{b}$ 適合此式.

證: 顯然只須考慮 ξ 爲無理數之情形. 設 $\frac{a_n}{b_n}$, $\frac{a_n'}{b_n'}$ 爲 $\mathfrak{F}_n$ 中適合

$$\frac{a_n}{b_n}<\xi<\frac{a_n'}{b_n'}$$

之二鄰項,則由定理 5 之證明,其中必有一適合 (2) 式. 由定理 1 卽得出我們的定理.

定理 8. 任與一無理數 ξ, 必有無數個有理數 $\frac{a}{b}$ 存在,使

$$\left|\xi-\frac{a}{b}\right|<\frac{1}{\sqrt{5}\,b^2}. \tag{3}$$

證：不失其普遍性，我們可以假定 $0<\xi<1$，作 n 級 Farey 貫．命 $\frac{a}{b}$ 及 $\frac{a'}{b'}$ 爲二鄰項，適合於

$$\frac{a}{b}<\xi<\frac{a'}{b'}$$

者．命 $\omega=b'/b$．今分兩種情況論之：

1）假定 $\omega>\frac{1}{2}(1+\sqrt{5})$ 或 $\omega<\frac{1}{2}(\sqrt{5}-1)$，則由定理 2，

$$\frac{a'}{b'}-\frac{a}{b}=\frac{1}{bb'}=\frac{1}{b^2\omega}.$$

由於

$$\frac{1}{\omega}-\frac{1}{\sqrt{5}}\left(1+\frac{1}{\omega^2}\right)=-\frac{1}{\sqrt{5}\,\omega^2}(\omega^2-\sqrt{5}\,\omega+1)=$$

$$=-\frac{1}{\sqrt{5}\,\omega^2}\left(\omega-\frac{1}{2}(\sqrt{5}+1)\right)\left(\omega-\frac{1}{2}(\sqrt{5}-1)\right)<0,$$

故
$$\frac{a'}{b'}-\frac{a}{b}<\frac{1}{\sqrt{5}\,b^2}\left(1+\frac{1}{\omega^2}\right)=\frac{1}{\sqrt{5}}\left(\frac{1}{b^2}+\frac{1}{b'^2}\right),$$

即
$$\frac{a}{b}+\frac{1}{\sqrt{5}}\frac{1}{b^2}>\frac{a'}{b'}-\frac{1}{\sqrt{5}}\frac{1}{b'^2}.$$

故 $\left(\frac{a}{b},\frac{a}{b}+\frac{1}{\sqrt{5}\,b^2}\right)$ 與 $\left(\frac{a'}{b'}-\frac{1}{\sqrt{5}\,b'^2},\frac{a'}{b'}\right)$ 中有一部分相重合，因而必有一包有 ξ，即有

$$\left|\xi-\frac{a}{b}\right|<\frac{1}{\sqrt{5}\,b^2},\quad 或\quad \left|\xi-\frac{a'}{b'}\right|<\frac{1}{\sqrt{5}\,b'^2};\tag{4}$$

2）假定 $\frac{1}{2}(1+\sqrt{5})>\omega>\frac{1}{2}(\sqrt{5}-1)$．則

$$b+b'>\frac{1}{2}(\sqrt{5}+1)\,b,\qquad b+b'<\frac{1}{2}(\sqrt{5}+1)\,b'.$$

故對於隔間 $\left(\frac{a}{b},\frac{a+a'}{b+b'}\right)$ 及 $\left(\frac{a+a'}{b+b'},\frac{a'}{b'}\right)$ 皆可用 1）之方法．因而得出三種可能性之一．即除（4）之兩種情形外，還可能有

$$\left|\xi-\frac{a+a'}{b+b'}\right|<\frac{1}{\sqrt{5}\,(b+b')^2}.$$

由於對一固定之 n，必有一組 a,b 適合於（3），由於 ξ 爲無理數，由定理

1, b 及 b' 隨 n 趨於無窮. 故得定理.

習題. 證明二鄰項之分母不同.

§ 11. Виноградов 關於函數的分數部分和的估値定理.

以 $\{\alpha\}$ 表示 α 之分數部分,卽 $\{\alpha\}=\alpha-[\alpha]$. 本節的目的在於研究形如

$$\sum_{A\leqslant x<B}\{f(x)\}$$

的和. 其應用見下節.

定理 1. 設 $m>0$, $(a, m)=1$, $h\geqslant 0$, c 爲實數. 並假定當 $x=0,\cdots,m$ 時,常有 $c\leqslant\psi(x)\leqslant c+h$. 命

$$S=\sum_{x=0}^{m-1}\left\{\frac{ax+\psi(x)}{m}\right\}.$$

則

$$\left|S-\frac{1}{2}m\right|\leqslant h+\frac{1}{2}.$$

證: 顯然有

$$\left|S-\frac{1}{2}m\right|\leqslant\sum_{x=0}^{m-1}\left|\left\{\frac{ax+\psi(x)}{m}\right\}-\frac{1}{2}\right|\leqslant\frac{1}{2}m.$$

故當 $m\leqslant 2h+1$ 時,本定理顯然眞實.

今假定 $m>2h+1$. 命 r 爲 $ax+[c]$ 對模 m 的最小正剩餘. 顯然有

$$S=\sum_{r=0}^{m-1}\left\{\frac{r+\Phi(r)}{m}\right\},\tag{1}$$

此處

$$\Phi(r)=\psi(x)-[c].$$

故得

$$\{c\}\leqslant\Phi(r)\leqslant\{c\}+h.\tag{2}$$

若 $0\leqslant r<m-[h+\{c\}]$, 則

$$0\leqslant\{c\}\leqslant r+\Phi(r)\leqslant m-[h+\{c\}]-1+\{c\}+h<m,$$

卽

$$0\leqslant\frac{r+\Phi(r)}{m}<1,$$

故

$$\left\{\frac{r+\Phi(r)}{m}\right\}=\frac{r+\Phi(r)}{m},$$

卽得

$$\frac{r}{m}+\frac{\{c\}}{m}\leqslant\left\{\frac{r+\Phi(r)}{m}\right\}\leqslant\frac{r}{m}+\frac{\{c\}+h}{m}. \tag{3}$$

若 $m-[h+\{c\}]\leqslant r<m$, 命 $r=m-s$, 則 $s=1,2,\cdots,[h+\{c\}]$. 故得

$$\left\{\frac{r+\Phi(r)}{m}\right\}=\left\{1+\frac{\Phi(r)-s}{m}\right\}.$$

當 $\Phi(r)-s\geqslant 0$, 則由 $\Phi(r)-s\leqslant h+\{c\}-1<m$, 可知

$$\frac{\{c\}-s}{m}\leqslant\left\{\frac{r+\Phi(r)}{m}\right\}=\frac{\Phi(r)-s}{m}\leqslant\frac{h+\{c\}-s}{m}; \tag{4}$$

又若 $\Phi(r)-s<0$, 則由 $0<m+\{c\}-s\leqslant r+\Phi(r)<m$, 可知

$$\frac{r+\{c\}}{m}\leqslant\left\{\frac{r+\Phi(r)}{m}\right\}=\frac{r+\Phi(r)}{m}\leqslant\frac{r+h+\{c\}}{m}. \tag{5}$$

總括 (4),(5) 二式,可知

$$-1+\frac{r}{m}+\frac{\{c\}}{m}\leqslant\left\{\frac{r+\Phi(r)}{m}\right\}\leqslant\frac{r}{m}+\frac{h+\{c\}}{m}. \tag{6}$$

綜合 (3) 及 (6) 可知

$$\{c\}-(h+\{c\})\leqslant S-\sum_{r=0}^{m-1}\frac{r}{m}\leqslant h+\{c\},$$

因此得出

$$-h\leqslant S-\frac{1}{2}(m-1)\leqslant h+1.$$

故得定理.

定理 2. 設 m 爲整數, $A>2$, $1\leqslant m\leqslant A^{\frac{1}{3}}$, $(a,m)=1$, $k\geqslant 1$. 又設

$$S=\sum_{x=M}^{M+m-1}\{f(x)\},$$

此處 $f(x)$ 在 $M\leqslant x\leqslant M+m-1$ 中定義,並有二級連續導數,且滿足於

$$f'(M)=\frac{a}{m}+\frac{\theta}{m^2},\qquad (a,m)=1,\quad |\theta|<1,$$

$$\frac{1}{A} \leqslant |f''(x)| \leqslant \frac{k}{A},$$

則

$$\left|S-\frac{1}{2}m\right| \leqslant \frac{1}{2}(k+5).$$

證: 由廣義中值公式可知

$$f(M+y)=f(M)+y\,f'(M)+\frac{y^2}{2}f''(M+\theta' y), \quad |\theta'|<1.$$

在定理 1 中取

$$\psi(y)=m\left(f(M)+\frac{\theta}{m^2}y+\frac{1}{2}y^2 f''(M+\theta' y)\right).$$

由於 $f''(x)$ 的連續性及 $|f''(x)|>\frac{1}{A}$，可知其不變號．不妨假定 $f''(x)>0$. 則

$$m\left(f(M)-\frac{m}{m^2}\right)<\psi(y)<m\left(f(M)+\frac{m}{m^2}+\frac{1}{2}\frac{m^2}{A}k\right).$$

即得

$$m\,f(M)-1<\psi(y)<m\,f(M)+1+\frac{1}{2}k.$$

即在定理 1 中可取 $c=mf(M)-1$, $h=2+\frac{1}{2}k$.

定理 3. 設 $k\geqslant 1$, $f(x)$ 在區間 $M\leqslant x\leqslant M+m$ 內定義並有連續之二級導數，且

$$\frac{1}{A} \leqslant |f''(x)| \leqslant \frac{k}{A}.$$

則

$$S=\sum_{x=M}^{M+m-1}\{f(x)\}=\frac{1}{2}m+O(\Delta),$$

此處

$$\Delta=(k^2 m\log A+kA)A^{-\frac{1}{3}}.$$

證: 取 $\tau=A^{\frac{1}{3}}$, $M=M_1$, 由定理 10.6 可知有 a_1, m_1, θ_1 存在，使

$$f'(M_1)=\frac{a_1}{m_1}+\frac{\theta_1}{m_1\tau}, \qquad 0<m_1\leqslant\tau, (a_1, m_1)=1, |\theta_1|<1. \tag{7}$$

由定理 2 可知

$$\sum_{x=M_1}^{M_1+m_1-1}\{f(x)\} = \frac{1}{2}m_1 + \frac{\theta_1'}{2}(k+5), \qquad |\theta_1'| \leqslant 1.$$

取 $M_2 = M_1 + m_1$，再由定理 10.6 可知有 a_2, m_2, θ_2 存在，使

$$f'(M_2) = \frac{a_2}{m_2} + \frac{\theta_2}{m_2\tau}, \quad 0 < m_2 \leqslant \tau, \quad (a_2, m_2) = 1, \quad |\theta_2| < 1,$$

且有

$$\sum_{x=M_2}^{M_2+m_2-1}\{f(x)\} = \frac{1}{2}m_2 + \frac{\theta_2'}{2}(k+5), \qquad |\theta_2'| \leqslant 1.$$

繼行此法，若 s 步後有

$$0 \leqslant M + m - 1 - M_{s+1} < \tau,$$

則得

$$\left|S - \frac{1}{2}(m_1 + \cdots + m_s) - \frac{1}{2}(M + m - M_{s+1})\right| \leqslant$$

$$\leqslant \frac{s}{2}(k+5) + \frac{1}{2}(M + m - M_{s+1}),$$

卽（由於 $M_{s+1} = M + m_1 + \cdots + m_s$）

$$\left|S - \frac{1}{2}m\right| < \frac{1}{2}s(k+5) + \frac{1}{2}(\tau+1). \tag{8}$$

今往估計 s. 假定 $0<q<\tau$, $(p, q) = 1$. 若 p, q 已固定，今往估計 $m_1, \cdots, m_s$ 中有多少個等於 q. 由於 $f''(x)$ 的連續性及 $|f''(x)| > \frac{1}{A}$，可知在所討論之範圍內 $f''(x)$ 不變號. x 之適合於

$$\frac{p}{q} - \frac{1}{q\tau} \leqslant f'(x) \leqslant \frac{p}{q} + \frac{1}{q\tau} \tag{9}$$

者成一區間. 其中之任兩點 x_1, x_2 常有

$$-\frac{2}{q\tau} < f'(x_1) - f'(x_2) < \frac{2}{q\tau}.$$

卽得

$$\left|\int_{x_1}^{x_2} f''(t)\,dt\right| < \frac{2}{q\tau}.$$

卽得

$$\frac{1}{A}|x_2 - x_1| < \frac{2}{q\tau}.$$

故適合 (9) 式的 x 所成的區間的長度 $\leqslant \frac{2A}{q\tau}$. 故等於 q 的 m_i 的個數 $\leqslant$ $\leqslant \frac{2A}{q^2\tau}+1$.

其次，若 q 固定，今往求適合 (9) 之 p 的個數. 假定 $p_1>p_2$, 及

$$\frac{p_1}{q}-\frac{1}{q\tau}\leqslant f'(x_1)\leqslant\frac{p_1}{q}+\frac{1}{q\tau},$$

$$\frac{p_2}{q}-\frac{1}{q\tau}\leqslant f'(x_2)\leqslant\frac{p_2}{q}+\frac{1}{q\tau},$$

則得

$$\left|\int_{x_2}^{x_1} f''(t)\,dt\right| = |f'(x_1)-f'(x_2)| \geqslant \frac{p_1-p_2}{q}-\frac{2}{q\tau}.$$

卽得

$$\frac{mk}{A}\geqslant |x_1-x_2|\cdot\frac{k}{A}\geqslant\frac{p_1-p_2}{q}-\frac{2}{q\tau}.$$

卽得

$$p_1-p_2+1\leqslant\frac{kmq}{A}+\frac{2}{\tau}+1.$$

卽 p 的個數 $\leqslant \frac{kmq}{A}+\frac{2}{\tau}+1$.

總之，將諸 $f'(M_i)$ 寫成 (7) 之形式，諸分數 $\frac{a_i}{m_i}$ 中，其分母 m_i 爲 q 者的個數

$$\leqslant\left(\frac{2A}{q^2\tau}+1\right)\left(\frac{kmq}{A}+\frac{2}{\tau}+1\right)=$$

$$=\frac{km}{\tau}\left(\frac{2}{q}+\frac{q}{\tau^2}\right)+\left(\frac{2A}{q^2\tau}+1\right)\left(1+\frac{2}{\tau}\right).$$

將 $q=1,2,\cdots,[\tau]$ 相加，可知

$$s\leqslant\frac{km}{\tau}\left(2\log\tau+2+\frac{\tau^2+\tau}{2\tau^2}\right)+O\left(\frac{A}{\tau}\right)=$$

$$=O\left(\frac{km}{\tau}\log A+\frac{A}{\tau}\right).$$

代入 (8) 式可得定理.

§12. Виноградов 定理對整點問題之應用.

在定理 9.1 中已經證明：圓

$$u^2+v^2\leqslant x$$

中的整點數爲

$$R(x) = \pi x + O(\sqrt{x}).$$

本節之目的在於證明一更精密的定理:

定理 1 (Sierpinski). 設 $x \geqslant 2$, 則

$$R(x) = \pi x + O(x^{\frac{1}{3}} \log x).$$

此結果並非關於此問題的最好紀錄, 運用較複雜的分析工具, 著者在 1942 年證明 $R(x)=\pi x+O(x^{\frac{13}{40}+\epsilon})$. 但一般的推測爲 $R(x) = \pi x + O(x^{\frac{1}{4}+\epsilon})$. 此乃數論上的一個著名難題. 在證明定理 1 之前需要次之引理:

定理 2. 設 $f(x)$ 在區間 $Q \leqslant x \leqslant R$ 內具有二次連續導數,又設

$$\sigma(x) = \int_0^x \left(\frac{1}{2} - \{t\}\right) dt.$$

則

$$\sum_{Q<x\leqslant R} f(x) = \int_Q^R f(x)\, dx + \left(\frac{1}{2} - \{R\}\right) f(R) - \left(\frac{1}{2} - \{Q\}\right) f(Q) - \sigma(R) f'(R) +$$

$$+ \sigma(Q) f'(Q) + \int_Q^R \sigma(x) f''(x)\, dx.$$

證: 設 x_1 爲整數, $Q \leqslant \alpha < \beta \leqslant R$, $x_1 < \alpha < \beta < x_1 + 1$, 則由部分積分,我們有

$$-\int_\alpha^\beta f(x)\, dx = \int_\alpha^\beta f(x) \frac{d}{dx}\left(\frac{1}{2} - \{x\}\right) dx =$$

$$= \left(\frac{1}{2} - \{\beta\}\right) f(\beta) - \left(\frac{1}{2} - \{\alpha\}\right) f(\alpha) - \sigma(\beta) f'(\beta) + \sigma(\alpha) f'(\alpha) +$$

$$+ \int_\alpha^\beta \sigma(x) f''(x)\, dx. \tag{1}$$

命 $\alpha \to x_1$, $\beta \to x_1 + 1$, 則得

$$-\int_{x_1}^{x_1+1} f(x)\, dx = -\frac{1}{2} f(x_1+1) - \frac{1}{2} f(x_1) + \int_{x_1}^{x_1+1} \sigma(x) f''(x)\, dx.$$

由是卽得

$$-\int_{[Q]+1}^{[R]} f(x)\, dx = -\sum_{[Q]+1\leqslant x\leqslant [R]} f(x) + \frac{1}{2} f([Q]+1) + \frac{1}{2} f([R]) +$$

$$+\int_{[Q]+1}^{[R]}\sigma(x)\,f''(x)\,dx. \tag{2}$$

若在 (1) 中，命 $\alpha=Q$，$\beta\to[Q]+1$，則得

$$-\int_{Q}^{[Q]+1} f(x)\,dx=\frac{-1}{2}f([Q]+1)-\left(\frac{1}{2}-\{Q\}\right)f(Q)+\sigma(Q)\,f'(Q)+$$

$$+\int_{Q}^{[Q]+1}\sigma(x)\,f''(x)\,dx. \tag{3}$$

同理，有

$$-\int_{[R]}^{R} f(x)\,dx=\left(\frac{1}{2}-\{R\}\right)f(R)-\frac{1}{2}f([R])-\sigma(R)\,f'(R)+$$

$$+\int_{[R]}^{R}\sigma(x)\,f''(x)\,dx. \tag{4}$$

將 (2)，(3) 及 (4) 相加，卽得所求之公式.

定理 1 之證明： 由圓之圖像，顯然可以看出

$$R(x)=1+4\,[\sqrt{x}\,]+8\sum_{0<u\leq\sqrt{\frac{x}{2}}}[\sqrt{x-u^2}]-4\left[\sqrt{\frac{x}{2}}\right]^2. \tag{5}$$

顯然有

$$\sum_{0<u\leq\sqrt{\frac{x}{2}}}[\sqrt{x-u^2}\,]=\sum_{0<u\leq\sqrt{\frac{x}{2}}}\sqrt{x-u^2}-\sum_{0<u\leq\sqrt{\frac{x}{2}}}\{\sqrt{x-u^2}\,\}=$$

$$=\sum\nolimits_1-\sum\nolimits_2.$$

我們來估計 $\sum_1$. 取 $f(u)=\sqrt{x-u^2}$，則由定理 2，卽得

$$\sum\nolimits_1=\int_0^{\sqrt{\frac{x}{2}}}\sqrt{x-u^2}\,du+\left(\frac{1}{2}-\left\{\sqrt{\frac{x}{2}}\right\}\right)\sqrt{\frac{x}{2}}-\frac{1}{2}\sqrt{x}+\sigma\left(\sqrt{\frac{x}{2}}\right)-$$

$$-x\int_0^{\sqrt{\frac{x}{2}}}\frac{\sigma(u)\,du}{(x-u^2)^{3/2}}=\frac{\pi}{8}x+\frac{x}{4}+\left(\frac{1}{2}-\left\{\sqrt{\frac{x}{2}}\right\}\right)\sqrt{\frac{x}{2}}-\frac{1}{2}\sqrt{x}+O(1).$$

由上節定理 3，我們有

$$\sum\nolimits_2=\frac{1}{2}\sqrt{\frac{x}{2}}+O(x^{\frac{1}{3}}\log x).$$

將此結果代入 (5)，立得我們的定理.

與圓內整點問題相仿有 Dirichlet 除數問題. 前已證明

$$\sum_{1 \leqslant n \leqslant \xi} d(n) = \xi \log \xi + (2\gamma - 1)\xi + O(\xi^{\frac{1}{2}+\varepsilon}).$$

(定理 5.4). 今往證:

定理 3 (Вороной). 若 $\xi \geqslant 2$, 則

$$\sum_{1 \leqslant n \leqslant \xi} d(n) = \xi \log \xi + (2\gamma - 1)\xi + O(\xi^{\frac{1}{3}} \log^2 \xi)$$

關於此方面最好紀錄是遲宗陶君用閔嗣鶴先生建議的方法而獲得的，以 $O(\xi^{\frac{15}{46}+\varepsilon})$ 代替以上的 $O(\xi^{\frac{1}{3}} \log^2 \xi)$. 一般猜測最佳之結果應當為 $O(\xi^{\frac{1}{4}+\varepsilon})$.

證: 由定理 5.4 之證明，我們有

$$\sum_{1 \leqslant n \leqslant \xi} d(n) = 2 \sum_{1 \leqslant u \leqslant \sqrt{\xi}} \left[\frac{\xi}{u}\right] - [\sqrt{\xi}]^2. \tag{6}$$

取 $f(u) = \dfrac{1}{u}$，則由定理 2 即得

$$\sum_{1 \leqslant u \leqslant \sqrt{\xi}} \frac{1}{u} = \lim_{\varepsilon \to 0} \sum_{1-\varepsilon < u \leqslant \sqrt{\xi}} \frac{1}{u} = \int_1^{\sqrt{\xi}} \frac{du}{u} + \left(\frac{1}{2} - \{\sqrt{\xi}\}\right)\xi^{-\frac{1}{2}} +$$

$$+ \frac{1}{2} + \sigma(\sqrt{\xi})\,\xi^{-1} + 2\int_1^{\sqrt{\xi}} \sigma(x)\, x^{-3}\, dx.$$

注意

$$\int_1^{\infty} \sigma(x)\, x^{-3}\, dx = \frac{1}{2}\int_1^{\infty} \left(\frac{1}{2} - \{x\}\right) x^{-2}\, dx =$$

$$= \frac{1}{4} - \frac{1}{2}\sum_{n=1}^{\infty} \int_0^1 \frac{x}{(n+x)^2}\, dx =$$

$$= \frac{1}{4} - \frac{1}{2}\sum_{n=1}^{\infty} \left\{\log(n+1) - \log n - \frac{1}{n+1}\right\} =$$

$$= -\frac{1}{4} + \frac{1}{2}\gamma,$$

則得

$$2\sum_{1 \leqslant u \leqslant \sqrt{\xi}} \frac{\xi}{u} = \xi \log \xi + 2\left(\frac{1}{2} - \{\sqrt{\xi}\}\right)\xi^{\frac{1}{2}} + 2\gamma\xi + O(1). \tag{7}$$

我們現來估計

$$S=\sum_{1\leqslant u\leqslant\sqrt{\xi}}\left\{\frac{\xi}{u}\right\}.$$

取 t_0, 使 $[\sqrt{\xi}]2^{-t_0}\geqslant 2\,\xi^{\frac{1}{3}}\geqslant[\sqrt{\xi}]\,2^{-t_0-1}$, 則顯然有

$$S=\sum_{t=0}^{t_0}\sum_{[\sqrt{\xi}]2^{-t-1}\leqslant u\leqslant[\sqrt{\xi}]2^{-t}}\left\{\frac{\xi}{u}\right\}+O(\xi^{\frac{1}{3}}).$$

由上節定理 3, 卽得 (以 $[\sqrt{\xi}]\,2^{-t-1}$ 代 m, 以 $[\sqrt{\xi}]^3\xi^{-1}\,2^{-(3t+1)}$ 代 A),

$$\sum_{[\sqrt{\xi}]2^{-t-1}\leqslant u\leqslant[\sqrt{\xi}]2^{-t}}\left\{\frac{\xi}{u}\right\}=\frac{1}{2^{t+2}}\,[\sqrt{\xi}\,]+O\,(\xi^{\frac{1}{3}}\log\xi).$$

故

$$S=\frac{1}{2}\,[\sqrt{\xi}\,]+O(\xi^{\frac{1}{3}}\,\log^2\xi). \tag{8}$$

注意 $[\sqrt{\xi}\,]^2=\xi-2\,\{\sqrt{\xi}\,\}\,\xi^{\frac{1}{2}}+O(1)$, 則由 (6),(7) 及 (8),卽得定理.

§ 13. Ω-結果.

數論中不少著名問題皆在於估計某一表達式之精確度, 卽在於將誤差項之無窮大之階儘可能地降低. 此類結果通常稱之爲 O-結果. 上節定理 1 及定理 3 皆其例也. 另一方面, 吾人也常從事誤差不能再好的估計. 卽其無窮大之階不能好過如何情況之研究,此類結果稱爲 Ω-結果.

上節中曾提及定理 12.1 之 O-項一般推測最好的結果是 $O(x^{\frac{1}{4}+\varepsilon})$. 本節之目的在於證明. 對任一正數 $\varepsilon>0$, 不可能有以下之式子

$$R(x)=\pi x+O(x^{\frac{1}{4}-\varepsilon}).$$

但以下之結果較此略爲廣泛.

本節中之 K, K_1, K_2, K_3 皆表絕對常數. 可表示之數值可能因地而異, 卽同一符號不一定就代表同一數值,但這絕不會因此而發生誤解.

定理 1. 設 $c>0$, $a_1, a_2, \cdots$ 表一整數列,適合於

$$0\leqslant a_1\leqslant a_2\leqslant\cdots.$$

以 $f(n)$ 表 $a_i+a_j=n$ 之解答數. $r(x)=\sum_{n\leqslant x}f(n)$ 表適合於 $a_i+a_j\leqslant x$ 的 a_i, a_j 之數對的數目. 如是則

$$r(x) = cx + o(x^{\frac{3}{4}} \log^{-\frac{1}{2}} x) \tag{1}$$

决不能成立。

在證明本定理之前,先引進以下各引理:

定理 2. 設 a_n 爲實數,

$$\psi(\theta) = \sum_{n=-\infty}^{\infty} a_n e^{in\theta}.$$

一致收斂,且 $\sum_{n=-\infty}^{\infty} a_n^2$ 收斂,則

$$\frac{1}{2\pi}\int_{-\pi}^{\pi} |\psi(\theta)|^2 d\theta = \sum_{n=-\infty}^{\infty} a_n^2$$

證: 顯然有

$$|\psi(\theta)|^2 = \sum_{n=-\infty}^{\infty}\sum_{m=-\infty}^{\infty} a_m e^{i(n-m)\theta}.$$

由 $-\pi$ 到 π 逐項求積分卽得所求.

定理 3. 設 $b_n \geqslant 0$, $\varphi(z) = \sum_{n=1}^{\infty} b_n z^n$ 當 $|z| < 1$ 時收斂,則對 $0 < \alpha < < \pi$, $z = re^{i\theta}$ $(0 < r < 1)$ 時,有次之不等式

$$\frac{1}{2\alpha}\int_{-\alpha}^{\alpha} |\varphi(z)|^2 d\theta \geqslant \frac{1}{6\pi}\int_{-\pi}^{\pi} |\varphi(z)|^2 d\theta.$$

證: 引進一個函數

$$q(\theta) = \begin{cases} 1 - \left|\dfrac{\theta}{\alpha}\right|, & \text{當 } |\theta| \leqslant \alpha, \\ 0, & \text{當 } \alpha < |\theta| \leqslant \pi. \end{cases}$$

如是則

$$\int_{-\alpha}^{\alpha} |\varphi(z)|^2 d\theta \geqslant \int_{-\pi}^{\pi} |q(\theta)|^2 |\varphi(z)|^2 d\theta =$$

$$= \sum_{m,n=1}^{\infty} b_n b_m r^{n+m} \int_{-\pi}^{\pi} |q(\theta)|^2 e^{i(n-m)\theta} d\theta.$$

當 $m \neq n$ 時,

$$\int_{-\pi}^{\pi} |q(\theta)|^2 e^{i(n-m)\theta} d\theta = 2\int_0^{\alpha}\left(1 - \frac{\theta}{\alpha}\right)^2 \cos(n-m)\theta d\theta =$$

$$= \frac{4}{\alpha(n-m)^2}\left(1 - \frac{\sin(n-m)\alpha}{\alpha(n-m)}\right) \geqslant 0,$$

而 $m=n$ 時,

$$\int_{-\pi}^{\pi}|q(\theta)|^2\,d\theta=\frac{2\alpha}{3},$$

故得出.

$$\int_{-\alpha}^{\alpha}|\varphi(z)|^2\,d\theta\geqslant\frac{2\alpha}{3}\sum_{n=1}^{\infty}b_n^2r^{2n}=\frac{\alpha}{3\pi}\int_{-\pi}^{\pi}|\varphi(z)|^2\,d\theta.$$

定理 4. 設 $|z|<1$. 命

$$(1-z)^{-r}=\sum_{n=0}^{\infty}\gamma_n z^n,$$

則有常數 c, C 存在,使

$$0<c<\frac{\gamma_n}{n^{r-1}}<C<\infty.$$

證: 由二項式定理立得

$$\gamma_n=\frac{r(r+1)\cdots(r+n-1)}{1\cdot 2\cdot\cdots n}.$$

由於

$$\int_{\nu-\frac{1}{2}}^{\nu+\frac{1}{2}}\log t\,dt=\int_0^{\frac{1}{2}}\{\log(\nu+t)+\log(\nu-t)\}\,dt=$$

$$=\int_0^{\frac{1}{2}}\left\{\log\nu^2+\log\left(1-\frac{t^2}{\nu^2}\right)\right\}dt=$$

$$=\log\nu+O\left(\frac{1}{\nu^2}\right),$$

故得

$$\sum_{l=1}^{n}\log(r+l-1)=\sum_{l=1}^{n}\int_{r+l-\frac{3}{2}}^{r+l-\frac{1}{2}}\log t\,dt+O\left(\sum_{l=1}^{n}\frac{1}{(r+l-1)^2}\right)=$$

$$=\int_{r-\frac{1}{2}}^{r-\frac{1}{2}+n}\log t\,dt+O(1)=$$

$$=\left(r-\frac{1}{2}+n\right)\log\left(r-\frac{1}{2}+n\right)-\left(r-\frac{1}{2}+n\right)+O(1)=$$

$$=\left(r-\frac{1}{2}+n\right)\log n-n+O(1)$$

及

$$\log n! = \sum_{l=1}^{n} \log l = \left(\frac{1}{2} + n\right) \log n - n + O(1).$$

因此

$$\log \gamma_n = (r-1) \log n + O(1),$$

故得定理.

定理 5. 若 $b_n = o(n^{1/2} \log^{-1} n)$, 則當 $0 < r < 1$ 時,

$$\sum_{n=0}^{\infty} b_n r^n = o\left((1-r)^{-\frac{3}{4}} \log^{-1} \frac{1}{1-r}\right).$$

證: 由假定可知

$$\sum_{n=0}^{\infty} b_n r^n \leqslant K \sum_{n \leqslant (1-r)^{-\frac{1}{2}}} n^{\frac{1}{2}} r^n + \varepsilon_1(r) \log^{-1} \frac{1}{1-r} \sum_{n > (1-r)^{-\frac{1}{2}}} n^{\frac{1}{2}} r^n,$$

此處當 $r \to 1$ 時 $\varepsilon_1(r) \to 0$. 第一分和的項數 $\leqslant (1-r)^{-1/2}$ 每一項皆 $\leqslant (1-r)^{-1/4}$, 故此分和 $\leqslant (1-r)^{-3/4}$. 由定理 4, 第二分和

$$\leqslant \varepsilon_1(r) \log^{-1} \frac{1}{1-r} \sum_{n=1}^{\infty} n^{\frac{1}{2}} r^n$$

$$\leqslant \varepsilon(r) \log^{-1} \frac{1}{1-r} (1-r)^{-\frac{3}{2}}.$$

總之可得

$$\sum_{n=1}^{\infty} b_n r^n \leqslant K (1-r)^{-\frac{3}{4}} + \varepsilon(r) \log^{-1} \frac{1}{1-r} (1-r)^{-\frac{3}{2}} =$$

$$= o\left(\log^{-1} \frac{1}{1-r} (1-r)^{-\frac{3}{2}}\right).$$

定理 6. 假定 $f(x)$, $g(x)$ 爲 (a, b) 間定義的實連續函數,則

$$\left|\int_a^b f(x)\, g(x)\, dx\right| \leqslant \left(\int_a^b f^2(x)\, dx \int_a^b g^2(x)\, dx\right)^{\frac{1}{2}}.$$

證: 設 λ 爲任一實數,因

$$\lambda^2 \int_a^b f^2(x)\, dx + 2\lambda \int_a^b f(x)\, g(x)\, dx + \int_a^b g^2(x)\, dx =$$

$$= \int_a^b (\lambda f(x) + g(x))^2\, dx \geqslant 0.$$

故上式右邊 λ 之二次式之判別式 $\leqslant 0$，卽得定理.

定理 1 之證明： 設 $\frac{1}{2}<r<1$，$z=re^{i\theta}$，$1-r<\alpha<\frac{\pi}{2}$．命

$$g(z)=\sum_{k=1}^{\infty} z^{a_k},$$

由此立得

$$g^2(z)=\sum_{n=0}^{\infty} f(n)\, z^n$$

及

$$(1-z)^{-1}\, g^2(z)=\sum_{n=0}^{\infty} r(n)\, z^n$$

若 (1) 式成立，則

$$(1-z)^{-1}\, g^2(z)=c\sum_{n=0}^{\infty} n\, z^n+h(z)=$$

$$=c\, z(1-z)^{-2}+h(z), \tag{2}$$

此處

$$h(z)=\sum_{n=0}^{\infty} v_n z^n, \qquad v_n=o\,(n^{\frac{3}{4}}\log^{-\frac{1}{2}} n).$$

今往導出矛盾.

由 (2) 可知

$$\int_{-\alpha}^{\alpha} |g(z)|^2\, d\theta=\int_{-\alpha}^{\alpha} |cz(1-z)^{-1}+(1-z)\, h(z)|\, d\theta\leqslant$$

$$\leqslant c\int_{-\pi}^{\pi} |1-z|^{-1}\, d\theta+\int_{-\alpha}^{\alpha} |1-z|\; |h(z)|\, d\theta, \tag{3}$$

由定理 2 及定理 4 可知

$$\int_{-\pi}^{\pi} |1-z|^{-1}\, d\theta=\int_{-\pi}^{\pi} |(1-z)^{-\frac{1}{2}}|^2\, d\theta<$$

$$<K\sum_{n=1}^{\infty}\frac{r^{2n}}{n}<K\log\frac{1}{1-r}.$$

又由定理 6, 5 可知

$$\int_{-\alpha}^{\alpha}|1-z|\,|h(z)|\,d\theta \leqslant \sqrt{\int_{-\alpha}^{\alpha}|1-z|^2\,d\theta\int_{-\alpha}^{\alpha}|h(z)|^2\,d\theta} \leqslant$$

$$\leqslant \sqrt{(2\alpha(1+r^2)-4r\sin\alpha)\int_{-\pi}^{\pi}|h(z)|^2\,d\theta} \leqslant$$

$$\leqslant \left\{(2\alpha(1-r)^2+4r(\alpha-\sin\alpha))\,\varepsilon(r)\,(1-r)^{-\frac{3}{2}}\log^{-1}\frac{1}{1-r}\right\}^{\frac{1}{2}} \leqslant$$

$$\leqslant \varepsilon(r)\,\alpha^{\frac{3}{2}}\,(1-r)^{-\frac{3}{4}}\,\log^{-\frac{1}{2}}\frac{1}{1-r},$$

此處當 $r\to 1$ 時 $\varepsilon(r)\to 0$. 故由 (3) 得

$$\int_{-\alpha}^{\alpha}|g(z)|^2\,d\theta \leqslant K_1\log\frac{1}{1-r}+\varepsilon(r)\,\alpha^{\frac{3}{2}}\,(1-r)^{-\frac{3}{4}}\,\log^{-\frac{1}{2}}\frac{1}{1-r}. \qquad (4)$$

另一方面,由定理 2 可知

$$\int_{-\alpha}^{\alpha}|g(z)|^2\,d\theta > \frac{\alpha}{3\pi}\int_{-\pi}^{\pi}|g(z)|^2\,d\theta = \frac{\alpha}{3\pi}\sum_{k=1}^{\infty}r^{2a_k} =$$

$$= \frac{\alpha}{3\pi}\,g(r^2).$$

由 (2) 及定理 4 可知

$$g^2(r^2) = c\,r^2(1-r^2)^{-1}+(1-r^2)\,h(r^2) =$$

$$= c\,r^2(1-r^2)^{-1}+(1-r^2)\,O(\sum n^{-\frac{1}{4}}r^{2n}) >$$

$$> K(1-r)^{-1}-O((1-r)^{1-\frac{5}{4}}) >$$

$$> K(1-r)^{-1}.$$

故得

$$\int_{-\alpha}^{\alpha}|g(z)|^2\,d\theta > K_2\,\alpha(1-r)^{-\frac{1}{2}}. \qquad (5)$$

取 $K_2\varepsilon^{-2/3} < 1+K_1$, 又命 $\alpha = \varepsilon^{-2/3}(1-r)^{1/2}\log\frac{1}{1-r}$, 則由 (4) 與 (5) 可得

$$K_2\,\varepsilon^{-2/3} < K_1+1$$

此乃一矛盾. 故定理已證明.

§ 14. Dirichlet 級數.

Dirichlet 級數乃是形如

$$F(s)=\sum_{n=1}^{\infty}\frac{f(n)}{n^s}$$

之級數，此 $F(s)$ 稱為 $f(n)$ 的演成函數.

本書並不討論 Dirichlet 級數的基本性質，而僅討論其若干形式上之變化而已. 甚且不說明級數之收斂範圍.

若 $f(n)$ 是一積性函數，則

$$F(s)=\prod_p\left(1+\frac{f(p)}{p^s}+\frac{f(p^2)}{p^{2s}}+\cdots\right),$$

此處 p 過所有的素數. 又若 $f(n)$ 是一完全積性函數，則

$$F(s)=\prod_p\left(1-\frac{f(p)}{p^s}\right)^{-1}.$$

若

$$G(s)=\sum_{n=1}^{\infty}\frac{g(n)}{n^s},$$

則

$$F(s)\ G(s)=\sum_{l=1}^{\infty}\frac{f(l)}{l^s}\sum_{m=1}^{\infty}\frac{g(m)}{m^s}=$$

$$=\sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{d|n}f(d)\,g\left(\frac{n}{d}\right).$$

故 $F(s)\ G(s)$ 乃

$$\sum_{d|n}f(d)\,g\left(\frac{n}{d}\right)$$

之演成函數. 由此可以說明定理 4.2.

命

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}.$$

此乃解析數論中著名的 Riemann ζ 函數，有乘積式

$$\zeta(s)=\prod_p\left(1-\frac{1}{p^s}\right)^{-1}. \tag{1}$$

故

$$\frac{1}{\zeta(s)}=\prod_p\left(1-\frac{1}{p^s}\right)=\prod_p\left(1+\frac{\mu(p)}{p^s}+\frac{\mu(p^2)}{p^{2s}}+\cdots\right)=$$

$$=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}. \tag{2}$$

若 $g(n)$ 是 $f(n)$ 之 Möbius 變換，則其演成函數 $G(s)$ 及 $F(s)$ 有次之關係

$$G(s)=\zeta(s)F(s).$$

Möbius 反轉定理實對應於

$$F(s)=\frac{1}{\zeta(s)}G(s).$$

又可知

$$\sum_{n=1}^{\infty}\frac{d(n)}{n^s}=\zeta^2(s). \tag{3}$$

更有

$$\sum_{n=1}^{\infty}\frac{|\mu(n)|}{n^s}=\prod_p\left(1+\frac{1}{p^s}\right)=\frac{\prod_p\left(1-\frac{1}{p^{2s}}\right)}{\prod_p\left(1-\frac{1}{p^s}\right)}=\frac{\zeta(s)}{\zeta(2s)}. \tag{4}$$

取 (1) 式之對數且微分之，則得

$$\frac{\zeta'(s)}{\zeta(s)}=-\sum_p\frac{\log p}{p^s}\left(1-\frac{1}{p^s}\right)^{-1}=$$

$$=-\sum_p\log p\sum_{m=1}^{\infty}\frac{1}{p^{ms}}=$$

$$=-\sum_{n=2}^{\infty}\frac{\Lambda(n)}{n^s}. \tag{5}$$

因爲

$$\zeta'(s)=-\sum_{n=2}^{\infty}\frac{\log n}{n^s}, \tag{6}$$

此二式重新建立了 $\log n$ 與 $\Lambda(n)$ 之 Möbius 變換關係。

$$\log\zeta(s)=-\sum_p \log\left(1-\frac{1}{p^s}\right)=$$

$$=\sum_p\sum_{m=1}^{\infty}\frac{1}{mp^{sm}}=\sum_{n=1}^{\infty}\frac{\Lambda_1(n)}{n^s}. \tag{7}$$

又

$$\zeta''(s)=\sum_{n=1}^{\infty}\frac{\log^2 n}{n^s}.$$

由於

$$\sum_{n=1}^{\infty}\frac{\Lambda(n)\log n}{n^s}=\left(\frac{\zeta'(s)}{\zeta(s)}\right)'$$

及

$$\sum_{n=1}^{\infty}\frac{1}{n^s}\left(\sum_{d|n}\Lambda(d)\,\Lambda\left(\frac{n}{d}\right)\right)=\left(\frac{\zeta'(s)}{\zeta(s)}\right)^2,$$

由

$$\frac{\zeta''(s)}{\zeta(s)}=\frac{d}{ds}\,\frac{\zeta'(s)}{\zeta(s)}+\left(\frac{\zeta'(s)}{\zeta(s)}\right)^2 \tag{8}$$

而得出

$$\sum_{d|n}\mu(d)\log^2\frac{n}{d}=\sum_{d|n}\Lambda(d)\,\Lambda\left(\frac{n}{d}\right)+\Lambda(n)\log n.$$

又 § 8 中之結果也可敍述爲：命

$$L(s)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s},$$

則

$$\sum_{n=1}^{\infty}\frac{r(n)}{n^s}=4\,L(s)\,\zeta(s). \tag{9}$$

解析數論之研究乃從 $F(s)$ 之解析性質入手，因而研究出數論函數 $f(n)$ 之性質。

習題 1. 討論 (1) — (9) 成立之範圍.

習題 2. 建立:

$$\frac{\zeta^3(s)}{\zeta(2s)} = \sum_{n=1}^{\infty} \frac{d(n^2)}{n^s}, \qquad (s > 1).$$

$$\frac{\zeta^4(s)}{\zeta(2s)} = \sum_{n=1}^{\infty} \frac{(d(n))^2}{n^s}, \qquad (s > 1).$$

$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s}, \qquad (s > 2).$$

$$\zeta(s)\,\zeta(s-a) = \sum_{n=1}^{\infty} \frac{\sigma_a(n)}{n^s}, \qquad s > \max(1, a+1).$$

$$\frac{\zeta(s)\,\zeta(s-a)\,\zeta(s-b)\,\zeta(s-a-b)}{\zeta(2s-a-b)} = \sum_{n=1}^{\infty} \frac{\sigma_a(n)\,\sigma_b(n)}{n^s},$$

$$s > \max(1, a+1, b+1, a+b+1).$$

§ 15. Lambert 級數.

定義.

$$F(x) = \sum_{n=1}^{\infty} f(n) \frac{x^n}{1-x^n} \qquad (1)$$

稱爲 Lambert 級數, $F(x)$ 稱爲 $f(n)$ 之演成函數.

把 (1) 展開成冪級數,則

$$F(x) = \sum_{n=1}^{\infty} f(n) \sum_{m=1}^{\infty} x^{mn} =$$

$$= \sum_{n=1}^{\infty} g(n)\, x^n,$$

此處

$$g(n) = \sum_{d|n} f(d).$$

故若 $y(n)$ 是 $f(n)$ 之 Möbius 變換,則以 $g(n)$ 爲係數之冪級數可以變爲 $f(n)$ 的 Lambert 演成函數.

今取 $g(n) = \Delta(n)$,則有

$$x = \sum_{n=1}^{\infty} \frac{\mu(n)\, x^n}{1-x^n}. \qquad (1)$$

又取 $g(n)=n$，則由

$$\sum_{n=1}^{\infty} nx^n = \frac{x}{(1-x)^2},$$

可知

$$\sum_{n=1}^{\infty} \frac{\varphi(n)\,x^n}{1-x^n} = \frac{x}{(1-x)^2}. \tag{2}$$

同法

$$\sum_{n=1}^{\infty} d(n)\,x^n = \frac{x}{1-x} + \frac{x^2}{1-x^2} + \frac{x^3}{1-x^3} + \cdots. \tag{3}$$

$$\sum_{n=1}^{\infty} r(n)\,x^n = 4\left(\frac{x}{1-x} - \frac{x^3}{1-x^3} + \frac{x^5}{1-x^5} - \cdots\right). \tag{4}$$

第　七　章

三角和及特徵

§1. 剩餘系之表示法.

設 m 是一正整數,由前已知依模 m 可將整數分爲 m 個剩餘類:

$$A_0, A_1, \cdots, A_{m-1}$$

(其中 A_s 包括所有的 $\equiv s \pmod m$ 之整數). 此諸剩餘類之間可以定義加法,即

$$A_s + A_t = A_u, \qquad u = \begin{cases} s+t & 若\ s+t<m, \\ s+t-m & 若\ s+t \geqslant m. \end{cases}$$

此乃所謂"羣"之性質. 在羣論中有所謂表示論 (representation theory) 者,乃將一較抽象之對象表成具體的事物,此種方法極爲有用(如量子力學). 在本節中將討論剩餘類之加法羣之表示法.

對應於較抽象之概念類 A_u, 吾人有一複數 ξ_u, 使其間保持有相似之關係;即如

$$A_u + A_v = A_w, \tag{1}$$

則

$$\xi_u \xi_v = \xi_w. \tag{2}$$

在吾人眼前卽有一表示法:

$$\xi_u = e^{2\pi i u/m}.$$

此表示法之優點在於: (i) 同一類之數對應於一數,卽若 $u = v + km$, 則

$$\xi_u = e^{2\pi i(v+km)/m} = e^{2\pi i v/m} = \xi_v;$$

(ii) 若 $u + v \equiv w \pmod m$, 則

$$\xi_u \xi_v = \xi_w.$$

經此種方法表示後,類之加法之抽象概念一變而爲具體的複數之乘法矣. 因

此可以體會出同餘式方面之結果有可能從三角和之結果得出． 此卽三角和之研究在數論中佔重要地位之由來．

命 a 爲任一整數，則

$$\xi_u^a = e^{2\pi iau/m}$$

也有 (i) 及 (ii) 之性質． 所以共有 m 個不同之表示法。

今往證明舍此而外並無其他： 若 η_u 是任一複數有以上之性質者，則由 $mu \equiv 0 \pmod{m}$，可知

$$\eta_u^m = \eta_0.$$

但

$$\eta_0^2 = \eta_0,$$

故若 $\eta_0 \neq 0$，則 $\eta_0 = 1$． 由是 η_u 爲 1 之 m 次根． 如命

$$\eta_1 = e^{2\pi ia/m},$$

則

$$\eta_u = \eta_1^u = e^{2\pi iau/m}.$$

若 $\eta_0 = 0$，則 $\eta_u = 0$，卽恆等於零之表示法，不在討論之列。

定理 1. 依 m 整除 n 與否，可知

$$\frac{1}{m}\sum_{a=0}^{m-1} \xi_n^a = 1 \text{ 或 } 0,$$

卽

$$\frac{1}{m}\sum_{a=0}^{m-1} e^{2\pi ian/m} = 1 \text{ 或 } 0.$$

證： 若 $m|n$，則定理顯然． 若 $m \nmid n$，則

$$\sum_{a=0}^{m-1} \xi_n^a = \frac{1-\xi_n^m}{1-\xi_n} = 0.$$

由此定理可知，同餘式

$$f(x_1, \cdots, x_n) \equiv N \pmod{m}, \qquad 0 \leqslant x_\nu \leqslant m-1$$

之解答數可以表成

$$\frac{1}{m}\sum_{x_1=0}^{m-1} \cdots \sum_{x_n=0}^{m-1} \sum_{a=0}^{m-1} e^{2\pi ia(f(x_1, \cdots, x_n)-N)/m}.$$

經此法表達後,同餘式之問題獲得了解析形式.

對整數系統則有次之結果:

定理 2. 依 n 為 0 與否,可知

$$\int_0^1 e^{2\pi i n x}\,dx = 1 \text{ 或 } 0.$$

由此可以推出,方程

$$f(x_1, \cdots, x_n) = N, \qquad a_\nu \leqslant x_\nu \leqslant b_\nu$$

之整數解答之組數等於

$$\sum_{a_1 \leqslant x_1 \leqslant b_1} \cdots \sum_{a_n \leqslant x_n \leqslant b_n} \int_0^1 e^{2\pi i (f(x_1, \cdots, x_n) - N)\alpha}\,d\alpha.$$

例 1. Fermat 問題在證明: 當 $k \geqslant 3$ 時,

$$\int_0^1 \left(\sum_{x=1}^N e^{2\pi i x^k \alpha}\right)^2 \left(\sum_{x=1}^N e^{-2\pi i x^k \alpha}\right) d\alpha = 0.$$

例 2. Гольдбах 問題在證明

$$\int_0^1 \left(\sum_{p \leqslant 2N} e^{2\pi i p \alpha}\right)^2 e^{-4\pi i N \alpha}\,d\alpha > 0.$$

此二例子實質上並未給與我們對此二問題之解答以任何幫助.

習題 1. 設 $(n, m) = 1$,

$$S = \sum_{x=0}^{m-1} \sum_{y=0}^{m-1} \xi(x)\,\eta(y)\,e^{2\pi i x y n/m},$$

$$\sum_{x=0}^{m-1} |\xi(x)|^2 = X_0, \qquad \sum_{y=0}^{m-1} |\eta(x)|^2 = Y_0,$$

則

$$|S| \leqslant \sqrt{X_0 Y_0 m}.$$

§ 2. 特徵函數.

吾人已知一縮系對乘法也自封. 卽命

$$A_{a_1}, A_{a_2}, \cdots, A_{a_{\varphi(m)}}$$

表模 m 之剩餘類之適合於

$$(a_u, m) = 1$$

者. 則

$$A_{a_u} A_{a_v}$$

亦爲其中之一員. 今問其是否亦有表示法?

定義. 對模 m 之一特徵 $\chi(n)$ 是一僅當 $(n, m) = 1$ 時方有定義的函數, 且 $\chi(n)$ 適合於:

1) $\chi(1) \neq 0$;

2) 若 $a \equiv b \pmod{m}$, 則 $\chi(a) = \chi(b)$;

3) $\chi(ab) = \chi(a)\chi(b)$.

有時爲方便計,也加上: 若 $(n, m) > 1$, 則

$$\chi(n) = 0.$$

例. $\chi(n) = 1$ 顯然是一特徵,此名爲主特徵,以 χ_0 表之.

由定義可推得 $\chi(1) = 1$.

二特徵之積顯然爲一特徵, $\bar{\chi}(n)$ 也是一特徵.

先以 $m = p$ 爲一素數時爲例: 取 g 爲模 p 之一原根,則函數

$$\chi_a(n) = e^{2\pi i a \operatorname{ind} n/(p-1)}$$

卽爲一種表示法, 蓋其具有次之性質:

1) $\chi_a(1) = 1 \neq 0$;

2) 若 $n \equiv n' \pmod{p}$, 則

$$\operatorname{ind} n \equiv \operatorname{ind} n' \pmod{p-1},$$

故

$$\chi_a(n) = \chi_a(n');$$

3) $$\chi_a(nn') = e^{2\pi i a \operatorname{ind}(nn')/(p-1)} = \\ = e^{2\pi i a(\operatorname{ind} n + \operatorname{ind} n')/(p-1)} = \\ = \chi_a(n)\chi_a(n').$$

更具體些,當 p 爲奇素數時,取 $a = \frac{1}{2}(p-1)$,則

$$\chi_{\frac{1}{2}(p-1)}(n) = e^{\pi i \operatorname{ind} n} = \left(\frac{n}{p}\right).$$

是以二次剩餘之 Legendre 符號卽爲特徵之一. 由上可知關於模 p 共有 $p-1$ 個特徵. 不難證明也僅有 $p-1$ 個不同的特徵.

將此論據推廣到一般之情況:

1) $m = p^l$, p 是奇素數.

由定理 3.9.1, 對模 p^l 有原根存在, 因之若 $p \nmid n$, 也可以定義 ind n, 卽

$$n \equiv g^{\operatorname{ind} n} \pmod{p^l}.$$

如此可以獲得 $\varphi(p^l)$ 個特徵:

$$\chi_a(n) = e^{2\pi i a \operatorname{ind} n/\varphi(p^l)}, \qquad 1 \leqslant a \leqslant \varphi(p^l).$$

顯然有 $\chi_a(1) = 1$. 又有一特徵

$$\chi_1(n) = e^{2\pi i \operatorname{ind} n/\varphi(p^l)}$$

具次之性質: 若 $n \not\equiv 1 \pmod{p^l}$, 則

$$\chi_1(n) \neq 1.$$

2) $m = 2^l$.

2.1) $l = 1$, 僅有一主特徵.

2.2) $l = 2$, 舍主特徵外, 還有一特徵

$$\chi(1) = 1, \qquad \chi(3) = -1.$$

2.3) $l > 2$. 由定理 3.9.3, 當 n 爲一奇素數時, 吾人有一整數 b 使

$$n \equiv (-1)^{\frac{1}{2}(n-1)} 5^b \pmod{2^l}, \qquad b \geqslant 0.$$

吾人定義

$$\chi_{a,c}(n) = (-1)^{\frac{1}{2}(n-1)a} e^{2\pi i c b/2^{l-2}}.$$

這裏 a 有二不同値, mod 2, c 有 2^{l-2} 個不同値 mod 2^{l-2}, 故也給出了 $\varphi(2^l) = 2^{l-1}$ 個特徵. 而

$$\chi_{1,1}(n) = (-1)^{\frac{1}{2}(n-1)} e^{2\pi i b/2^{l-2}}$$

有次之性質: 若

$$\chi_{1,1}(n) = 1,$$

則 $n \equiv 1 \pmod{2^l}$ 或 $n \equiv -5^{2^{l-3}} \pmod{2^l}$. 當 $n \equiv -5^{2^{l-3}} \pmod{2^l}$ 時,

$$\chi_{0,1}(n) = -1 \neq 1.$$

卽若 $n \not\equiv 1 \pmod{2^l}$, 則可取一 $\chi_{a,c}$ 使

$$\chi_{a,c}(n) \neq 1.$$

3) 一般情況: 命

$$m = p_1^{l_1} \cdots p_s^{l_s}, \qquad l_\nu > 0,$$

是 m 的標準分解式.

對模 $p_\nu^{l_\nu}$ 之一特徵命爲

$$\chi^{(\nu)}(n),$$

則

$$\chi(n) = \prod_{\nu=1}^{s} \chi^{(\nu)}(n) \tag{1}$$

爲模 m 之一特徵. 由此可得 $\varphi(m)$ 個以 m 爲模之特徵.

反之,若特徵 $\chi(n)$ 之模爲

$$k = k_1 \cdots k_\nu,$$

此處 k_i 兩兩互素. 則存在以 $k_i(i = 1, \cdots, \nu)$ 爲模之特徵 $\chi_i(n)$ 使

$$\chi(n) = \chi_1(n) \cdots \chi_\nu(n).$$

欲明此理,祇需證明 $\nu = 2$ 之情形卽可.

由孫子定理,對任一 n, 吾人可定出 n_1 及 n_2 使

$$n_1 \equiv n \pmod{k_1}, \qquad n_1 \equiv 1 \pmod{k_2},$$
$$n_2 \equiv 1 \pmod{k_1}, \qquad n_2 \equiv n \pmod{k_2}.$$

定義

$$\chi_1(n) = \chi(n_1), \qquad \chi_2(n) = \chi(n_2),$$

不難證明 $\chi_1(n)$ 是一以 k_1 爲模之特徵, $\chi_2(n)$ 是一以 k_2 爲模之特徵. 由 n_1, n_2 之定義,可知

$$n_1 n_2 \equiv n \pmod{k_1}, \qquad n_1 n_2 \equiv n \pmod{k_2},$$

故

$$n_1 n_2 \equiv n \pmod{k}.$$

由是卽得

$$\chi(n) = \chi(n_1 n_2) = \chi(n_1)\chi(n_2) = \chi_1(n)\chi_2(n).$$

定理 1. 所造出的 $\varphi(m)$ 個特徵各不相同.

證: 若

$$\prod_{\nu=1}^{s} \chi^{(\nu)}(n) = \prod_{\nu=1}^{s} \chi_1^{(\nu)}(n).$$

由於 $\chi^{(\nu)}(n)/\chi_1^{(\nu)}(n)$ 也是對模 $p_\nu^{l_\nu}$ 之一特徵,故僅需證明：若

$$\prod_{\nu=1}^{s}\chi^{(\nu)}(n)$$

是主特徵,則 $\chi^{(\nu)}(n)$ 乃對模 $p_\nu^{l_\nu}$ 之主特徵.

取

$$n\equiv 1\ (\bmod p_\nu^{l_\nu}),\qquad 1\leqslant \nu\leqslant s-1,$$

$$n\equiv a\ (\bmod p_s^{l_s}),$$

則得出對所有的 a ($p_s\nmid a$) 常有

$$\chi^{(s)}(a)=1,$$

即 $\chi^{(s)}$ 是一主特徵, mod $p_s^{l_s}$. 故得出定理.

定理 2. 若 $n\not\equiv 1\ (\bmod m)$,則在此 $\varphi(m)$ 個特徵中可以選得一 $\chi(n)$ 使

$$\chi(n)\neq 1.$$

證: 由假定必有一素數 p_ν 使 $n\not\equiv 1\ (\bmod p_\nu^{l_\nu})$. 由前已知有一

$$\chi^{(\nu)}(n)\neq 1.$$

若 $\mu\neq\nu$, 取 $\chi^{(\mu)}(n)$ 爲主特徵,則

$$\chi(n)=\prod_{\nu=1}^{s}\chi^{(\nu)}(n)$$

即合所需.

定理 3.

$$\sum_n \chi(n)=\begin{cases}\varphi(m), & 若\quad \chi=\chi_0,\\ 0, & 若\quad \chi\neq\chi_0,\end{cases}$$

此和號過一完全剩餘系, mod m.

證: 當 $\chi=\chi_0$ 時此定理顯然正確.

當 $\chi\neq\chi_0$ 時,必有一整數 a 使 $(a,m)=1$ 且 $\chi(a)\neq 1$. 由

$$\chi(a)\sum_n\chi(n)=\sum_n\chi(an)=\sum_n\chi(n),$$

即

$$(\chi(a)-1)\sum_{n}\chi(n)=0,$$

故得定理.

定理 4. 命 c 表所有的特徵之總數,則

$$\sum_{\chi}\chi(n)=\begin{cases}c, & 若\ n\equiv 1\ (\bmod m),\\ 0, & 若\ n\not\equiv 1\ (\bmod m),\end{cases}$$

此和號過所有的特徵.

證: 因爲 $n^{\varphi(m)}\equiv 1\ (\bmod m)$,故

$$(\chi(n))^{\varphi(m)}=1.$$

故特徵之數有限,可以 c 表之.

若 $n\equiv 1\ (\bmod m)$,定理顯然正確,不必證明. 若 $n\not\equiv 1\ (\bmod m)$,由定理 2 有一特徵 $X(a)$ 使

$$X(n)\neq 1.$$

由

$$X(n)\sum_{\chi}\chi(n)=\sum_{\chi}X(n)\chi(n)=\sum_{\chi}\chi(n),$$

故

$$(X(n)-1)\sum_{\chi}\chi(n)=0.$$

卽得定理.

定理 5. 特徵總數等於 $\varphi(m)$.

換言之,上述之方法已將模 m 之所有特徵盡數列出,一個不少.

證: 由定理 3 及 4 可知

$$\sum_{n,\chi}\chi(n)=\begin{cases}\sum_{n}\sum_{\chi}\chi(n)=c,\\ \sum_{\chi}\sum_{n}\chi(n)=\varphi(m).\end{cases}$$

定義. (1) 式稱爲一特徵之標準分解式.

更肯定些,吾人命

$$\chi_1(n,2^l)=(-1)^{(n-1)/2},\quad \chi_2(n,2^l)=e^{2\pi ib/2^{l-2}}\quad (b\ 之意義見定理\ 3.9.3),$$

$$\chi(n,p^l)=e^{2\pi i\,\mathrm{ind}\,n/\varphi(p^l)}.$$

命 $m=2^a\prod_{p_\nu} p_\nu^{l_\nu}$ 爲 m 之標準分解式,則任一特徵 $\chi(n)$, mod m, 有次之分解式:

$$\chi(n)=\begin{cases}\prod_{p_\nu}(\chi(n,p_\nu^{l_\nu}))^{c_\nu}, & \text{若}\quad a=0,1,\\ (\chi_1(n,2^l))^{c_0}\prod_{p_\nu}(\chi(n,p_\nu^{l_\nu}))^{c_\nu}, & \text{若}\quad a=2,\\ (\chi_1(n,2^l))^{c_0}(\chi_2(n,2^l))^{c_0'}\prod_{p_\nu}(\chi(n,p_\nu^{l_\nu}))^{c_\nu}, & \text{若}\quad a\geqslant 3,\end{cases}$$

$$\left(c_0=0,\ 1,\qquad 0\leqslant c_0'<2^{l-2},\qquad 0\leqslant c_\nu<\varphi(p_\nu^{l_\nu})\right).$$

習題 1. 若 $\chi\neq\chi_0$, 則對任意的正整數 u 和 v $(v\geqslant u)$, 有

$$\left|\sum_{n=u}^{v}\chi(n)\right|\leqslant\frac{\varphi(m)}{2}.$$

習題 2. 若 $(l,m)=1$, 則

$$\sum_{\chi}\frac{\chi(n)}{\chi(l)}=\begin{cases}\varphi(m), & \text{當}\quad n\equiv l\ (\mathrm{mod}\ m),\\ 0, & \text{當}\quad n\not\equiv l\ (\mathrm{mod}\ m).\end{cases}$$

§3. 特徵之分類.

定義. $\chi(n)$ 名爲非原 (improper) 特徵, mod m, 如有 m 之因子 M, $M\neq m$, 具有次之性質: 當

$$n\equiv n'\ (\mathrm{mod}\ M),\qquad (n,m)=1,\qquad (n',m)=1$$

時,

$$\chi(n)=\chi(n').$$

無此性質之特徵謂之原 (primitive) 特徵.

例 1. 凡主特徵一定是非原特徵,因爲 $M=1$ 即適合定義之要求.

例 2. 若 $m=p$ 爲素數,則凡非主特徵皆爲原特徵.

例 3. 若 $m=p^l$ $(l>1)$ 爲奇素數之乘方,則特徵

$$\chi_a(n)=e^{2\pi i a\,\mathrm{ind}\,n/\varphi(m)}$$

爲非原特徵之必要且充分之條件爲 $p|a$. 故一非原特徵, mod p^l, 引出一特徵, mod p^{l-1}.

例 4. 若 $m=2^l$.

$l=1$ 時僅有主特徵. $l=2$ 時,非主特徵

$$\chi(1)=1, \qquad \chi(3)=-1$$

是原特徵.

當 $l\geqslant 3$ 時,若

$$\chi_{a,c}(n)=(-1)^{(n-1)a/2}\, e^{2\pi icb/2^{l-2}}$$

是非原特徵,則

$$\chi_{a,c}(n)=\chi_{a,c}(n+2^{l-1})$$

(且反之亦眞). 即

$$(-1)^{\frac{n-1}{2}a}\, e^{2\pi icb/2^{l-2}}=(-1)^{\frac{1}{2}a(n-1+2^{l-1})}\, e^{2\pi icb'/2^{l-2}}=$$
$$=(-1)^{\frac{1}{2}a(n-1)}\, e^{2\pi icb'/2^{l-2}},$$

即

$$c(b-b')\equiv 0 \qquad (\mathrm{mod}\ 2^{l-2}),$$

此處 b' 之定義是

$$n+2^{l-1}\equiv(-1)^{\frac{n-1}{2}}5^{b'} \qquad (\mathrm{mod}\ 2^{l}).$$

由於

$$\begin{aligned} n+2^{l-1} &\equiv n+n\,2^{l-1}\ (\mathrm{mod}\ 2^{l})\\ &\equiv n(1+2^{l-1})\ (\mathrm{mod}\ 2^{l})\\ &\equiv n\,5^{2^{l-3}} \qquad (\mathrm{mod}\ 2^{l}),\end{aligned}$$

故

$$b'\equiv b+2^{l-3} \qquad (\mathrm{mod}\ 2^{l-2}).$$

即 $\chi_{a,c}(n)$ 是原特徵之必要且充分條件爲 $2\nmid c$.

具體例子: $l=3$ 時

$$\chi_{a,c}(n)=(-1)^{\frac{n-1}{2}a+cb},$$

其中 $n=1, 3, 5, 7$ 時 $b=0, 1, 1, 0$. $c=1$ 時,

$$\chi_{a,1}(1)=1, \qquad \chi_{a,1}(3)=-(-1)^{a},$$
$$\chi_{a,1}(5)=-1, \qquad \chi_{a,1}(7)=(-1)^{a}$$

是原特徵. 可以簡寫爲 $\chi_{0,1}(n)=\left(\frac{2}{n}\right)$ 及 $\chi_{1,1}(n)=\left(\frac{-2}{n}\right)$. 而 $c=0$, $a=1$ 時,

$$\chi_{1,0}(1)=1, \qquad \chi_{1,0}(3)=-1,$$

$$\chi_{1,0}(5)=1, \qquad \chi_{1,0}(7)=-1$$

是一非原特徵，即 $\chi_{1,0}(n)=\left(\frac{-1}{n}\right)$.

在 §2 之表示法中，有

$$\chi(n)=\prod_{\nu}\chi^{(\nu)}(n).$$

若 $\chi^{(\nu)}(n)$ 中有一爲非原特徵，則 $\chi(n)$ 亦爲非原特徵. 反之，若 $\chi(n)$ 是非原特徵，則諸 $\chi^{(\nu)}(n)$ 中至少有一個是非原特徵.

再研究在何種情況時有實值的原特徵：如一特徵是實特徵，則其每一因子特徵也是實的. 當 p 是奇素數時，

$$(\chi(n,p^l))^{c_\nu}=e^{2\pi i c_\nu \operatorname{ind} n/\varphi(p^l)}$$

中之 c_ν 必須爲

$$\frac{1}{2}\varphi(p^l)$$

之倍數. 若該特徵又是原特徵，則由例 3, l 必須等於 1.

設

$$(\chi_2(n,2^l))^{c_0'}=e^{2\pi i c_0' b/2^{l-2}}$$

爲一實特徵，則必

$$2^{l-3}\mid c_0'.$$

若該特徵又是原特徵，則由例 4, 必須 $l\leqslant 3$. 故 $l>3$ 時不能有實的原特徵. $l=1$ 時，亦不能有原特徵，因若 $m=2m'$, $2\nmid m'$, 則由

$$n\equiv n' \pmod{m'}, \qquad (n,m)=1, \qquad (n',m)=1$$

得出

$$n\equiv n' \pmod{m},$$

即得 $\chi(n)=\chi(n')$, 故 $\chi(n)$ 非原特徵. 切實言之，能有實的原特徵的情況是

$$m\equiv 2^a p_1 p_2\cdots p_s,$$

此諸 p 乃不同之奇素數, $a=0, 2, 3$. 又既爲原特徵，就必須 $c_\nu=\frac{1}{2}\varphi(p)$, 即

$$(\chi(n,p))^{\frac{1}{2}(p-1)}=e^{\pi i \operatorname{ind} n}=\left(\frac{n}{p}\right).$$

故若 $a=0$, 其實原特徵即爲 Jacobi 符號

$$\left(\frac{n}{m}\right), \qquad (n, m) = 1.$$

若 $a = 2$，則實原特徵就是

$$(-1)^{\frac{n-1}{2}}\left(\frac{n}{m/4}\right), \qquad (n, m) = 1.$$

若 $a = 3$，則有兩種實原特徵:

$$(-1)^{\frac{1}{8}(n^2-1)}\left(\frac{n}{m/8}\right), \qquad (n, m) = 1,$$

及

$$(-1)^{\frac{n-1}{2}+\frac{n^2-1}{8}}\left(\frac{n}{m/8}\right) = (-1)^{\frac{1}{8}((n-2)^2-9)}\left(\frac{n}{m/8}\right), \qquad (n, m) = 1.$$

§4. 特徵和.

命

$$S(a, \chi) = \sum_{n=1}^{m} \chi(n)\, e^{2\pi i a n/m}.$$

定理 1. 若 $(m_1, m_2) = 1$，並把 χ 分解爲

$$\chi(n) = \chi_1(n)\, \chi_2(n),$$

此處 $\chi_1(n)$ 是 mod m_1，$\chi_2(n)$ 是 mod m_2 之特徵. 則

$$S(a, \chi) = \chi_1(m_2)\, \chi_2(m_1)\, S(a, \chi_1)\, S(a, \chi_2).$$

證: 命 $n = m_1 n_2 + m_2 n_1$. 則當 n_1, n_2 各過 mod m_1, mod m_2 之完全剩餘系時，n 也過 mod $m_1 m_2$ 之完全剩餘系. 故

$$S(a, \chi) = \chi_1(m_2)\, \chi_2(m_1) \sum_{n_1=1}^{m_1} \sum_{n_2=1}^{m_2} \chi_1(n_1)\, \chi_2(n_2)\, e^{2\pi i a(m_1 n_2 + m_2 n_1)/m_1 m_2} =$$

$$= \chi_1(m_2)\, \chi_2(m_1)\, S(a, \chi_1)\, S(a, \chi_2).$$

故對模 m 特徵和之研究一變而爲對以素數乘方爲模之特徵和之研究.

定理 2. 命 $m = p^l$. 若 $p|a$ 及 χ 是原特徵，或若 $p \nmid a$ 及 χ 是非原特徵（但若 $l = 1$，則 $\chi = \chi_0$ 之情況應除外），則

$$S(a, \chi) = 0.$$

證: 換變數，命

$$n = x\,(1 + p^{l-1} y),$$

則當 $1 \leqslant x \leqslant p^{l-1}$, $p \nmid x$ 及 $1 \leqslant y \leqslant p$ 時, n 過 mod p^l 之縮系;反之亦眞. 故得

$$S(a,\chi)=\sum_{\substack{x=1\\ p\nmid x}}^{p^{l-1}}\chi(x)\,e^{2\pi iax/p^l}\sum_{y=1}^{p}\chi(1+p^{l-1}y)\,e^{2\pi iaxy/p}.$$

若 $\chi(n)$ 非原特徵,則 $\chi(1+p^{l-1}y)=1$, 故得

$$S(a,\chi)=\begin{cases}0, & 若\ p\nmid a,\\ p\sum\limits_{x=1}^{p^{l-1}}\chi(x)\,e^{2\pi iax/p^l}, & 若\ p\mid a.\end{cases}$$

若 $\chi(n)$ 是原特徵,則必有一 u 使 $\chi(1+p^{l-1}u)\neq 1$; 而 $p|a$, 則由於

$$\chi(1+p^{l-1}u)\sum_{y=1}^{p}\chi(1+p^{l-1}y)=\sum_{y=1}^{p}\chi(1+p^{l-1}(y+u))=$$

$$=\sum_{y=1}^{p}\chi(1+p^{l-1}y).$$

卽得

$$\sum_{y=1}^{p}\chi(1+p^{l-1}y)=0,$$

也卽 $S(a,\chi)=0$.

此結果可以推廣成爲更普遍的形式:

定理 3. 若 $(m,a)=1$ 而 $\chi(n)$ 非原特徵 (但若 m 無平方因子,則 $\chi=\chi_0$ 之情況應除外) 或 $(m,a)>1$, 而 $\chi(n)$ 是原特徵,則 $S(a,\chi)=0$.

命

$$\tau(\chi)=S(1,\chi).$$

若 $(a,m)=1$, 則

$$\chi(a)\,S(a,\chi)=\sum_{n=1}^{m}\chi(an)e^{2\pi ian/m}=$$

$$=S(1,\chi).$$

定理 4. 命

$$C_q(n)=\sum_{(a,q)=1}e^{2\pi ian/q},$$

此處 a 過模 q 之一縮系,則

1) $C_q(n)$ 對 q 是積性函數,卽若 $(q_1,q_2)=1$, 則

$$C_{q_1}(n)\,C_{q_2}(n)=C_{q_1q_2}(n);$$

2)

$$C_{p^l}(n)=\begin{cases} p^l-p^{l-1}, & 若 \quad p^l\mid n, \\ -p^{l-1}, & 若 \quad p^l\nmid n,\quad p^{l-1}\mid n, \\ 0, & 若 \quad p^{l-1}\nmid n; \end{cases}$$

3)

$$C_q(1)=\mu(q).$$

證: 1) 之證明可由代換 $a=q_1a_2+q_2a_1$，並用前已熟知之方法得之. 由

$$C_{p^l}(n)=\sum_{a=1}^{p^l}e^{2\pi ian/p^l}-\sum_{a=1}^{p^{l-1}}e^{2\pi ian/p^{l-1}}$$

可得 2) 之證明.

3) 乃 1) 及 2) 之推理.

定理 5. 若 $\chi(n)$ 是原特徵,則

$$|\tau(\chi)|^2=m.$$

證: 今先討論 $m=p^l$ 之情況. 易見

$$|\tau(\chi)|^2=\tau(\chi)\,\bar{\tau}(\chi)=$$

$$=\sum_{n=1}^{p^l}\chi(n)\,e^{2\pi in/p^l}\sum_{q=1}^{p^l}\bar{\chi}(q)\,e^{-2\pi iq/p^l}=$$

$$=\sum_{n=1}^{p^l}\chi(n)\,e^{2\pi in/p^l}\sum_{q=1}^{p^l}\bar{\chi}(nq)\,e^{-2\pi inq/p^l}=$$

$$=\sum_{q=1}^{p^l}\bar{\chi}(q)\sum_{\substack{n=1\\ p\nmid n}}^{p^l}e^{2\pi i(1-q)n/p^l}.$$

若 $p^{l-1}\nmid(q-1)$,則由定理 4, 上式右邊內和等於 0. 故祇需討論 $p^{l-1}\mid(q-1)$ 之情況,即 $q=1+p^{l-1}u$, $0\leqslant u\leqslant p-1$ 之情況,此時易見

$$|\tau(\chi)|^2=p^l-p^{l-1}-\sum_{u=1}^{p-1}\bar{\chi}(1+p^{l-1}u)\,p^{l-1}=$$

$$=p^l-p^{l-1}\sum_{u=1}^{p}\bar{\chi}(1+p^{l-1}u).$$

但因爲 $\chi(n)$ 是原特徵，故必有一 v 存在，使 $\chi(1+p^{l-1}v)\neq 0,1$. 故 $\bar{\chi}(1+p^{l-1}v)\neq 0,1$. 由

$$\bar{\chi}(1+p^{l-1}v)\sum_{u=1}^{p}\bar{\chi}(1+p^{l-1}u)=\sum_{u=1}^{p}\bar{\chi}(1+p^{l-1}(u+v))=\sum_{u=1}^{p}\bar{\chi}(1+p^{l-1}u),$$

卽得

$$\sum_{u=1}^{p}\bar{\chi}(1+p^{l-1}u)=0.$$

故定理對於 $m=p^l$ 之情況已經證明. 對於一般的情況，由定理 1 立可得出.

一般言之，

$$\tau(\chi)=\varepsilon\sqrt{m},\qquad |\varepsilon|=1.$$

但如何定出 ε 實非易事.

下節中將就 χ 是實原特徵之情況定出 ε.

關於實原特徵，吾人所知可略多:

定理 6. 若 χ 是實原特徵，則對奇數 m 有

$$\tau(\chi)=\begin{cases}\pm\sqrt{m}, & 若\quad m\equiv 1\pmod 4,\\ \pm i\sqrt{m}, & 若\quad m\equiv 3\pmod 4.\end{cases}$$

證: 如定理 5 之證明: 若 $m=p$, 則

$$(\tau(\chi))^2=\sum_{q=1}^{p}\chi(q)\sum_{n=1}^{p-1}e^{2\pi i(1+q)n/p}=\chi(-1)\,p.$$

已知

$$\chi(-1)=\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}},$$

故得定理.

§5. Gauss 和.

三角和

$$S(n,m)=\sum_{x=0}^{m-1}e^{2\pi i x^2 n/m},\qquad (n,m)=1$$

乃著名之 Gauss 和. 上式之和號中 x 過任一完全剩餘系，mod m, 皆可.

定理 1. 若 $(m,m')=1$, 則

$$S(n,mm')=S(nm',m)\,S(nm,m').$$

證: 命 $x = my + m'z$, 則

$$S(n, mm') = \sum_{x=1}^{mm'} e^{2\pi i x^2 n/mm'} =$$

$$= \sum_{y=1}^{m'} \sum_{z=1}^{m} e^{2\pi i n(my+m'z)^2/mm'} =$$

$$= \sum_{y=1}^{m'} e^{2\pi i m n y^2/m'} \sum_{z=1}^{m} e^{2\pi i m' n z^2/m},$$

故得定理.

故 Gauss 和之計算祇要對 $m = p^l$ 是素數乘方之情況計算之卽可.

定理 2. 命

$$\delta = \begin{cases} 1, & \text{當 } p \text{ 爲奇素數,} \\ 2, & \text{當 } p = 2. \end{cases}$$

則當 $l \geqslant 2\delta$ 時

$$S(n, p^l) = p\, S(n, p^{l-2}).$$

證: 命

$$x = y + p^{l-\delta} z,$$

則由於 $2(l-\delta) \geqslant l$,

$$S(n, p^l) = \sum_{y=1}^{p^{l-\delta}} \sum_{z=1}^{p^\delta} e^{2\pi i (y+p^{l-\delta} z)^2 n/p^l} =$$

$$= \sum_{y=1}^{p^{l-\delta}} e^{2\pi i y^2 n/p^l} \cdot \sum_{z=1}^{p^\delta} e^{4\pi i y z n/p^\delta} =$$

$$= p^\delta \sum_{\substack{y=1 \\ p \mid y}}^{p^{l-\delta}} e^{2\pi i y^2 n/p^l} =$$

$$= p^\delta \sum_{x=1}^{p^{l-\delta-1}} e^{2\pi i x^2 n/p^{l-2}}.$$

當 $p > 2$ 時,此卽所求. 當 $p = 2$ 時,由於

$$p \sum_{x=1}^{p^{l-3}} e^{2\pi i x^2 n/p^{l-2}} = \sum_{x=1}^{p^{l-2}} e^{2\pi i x^2 n/p^{l-2}},$$

故亦得所需.

由此定理可知 Gauss 和之計算重點落在計算

$$S(n,2), \quad S(n,4), \quad S(n,8)$$

及

$$S(n,p), \quad p \text{ 是奇素數.}$$

定理 3. 若 $2 \nmid n$, 則

$$S(n,2)=0,$$
$$S(n,4)=2(1+i^n),$$
$$S(n,8)=4e^{\frac{\pi i}{4}n}.$$

證: 顯然有

$$S(n,2)=1+e^{\frac{2\pi i}{2}n}=1-1=0,$$

$$S(n,4)=1+e^{\frac{2\pi i}{4}n}+e^{\frac{2\pi i}{4}4n}+e^{\frac{2\pi i}{4}9n}=$$
$$=1+i^n+1+i^n=2(1+i^n),$$

$$S(n,8)=2(1+e^{\frac{2\pi i}{8}n}+e^{\frac{2\pi i}{8}4n}+e^{\frac{2\pi i}{8}9n})=$$
$$=4e^{\frac{\pi i}{4}n}.$$

定理 4. 若 p 是奇素數,則

$$S(n,p)=\left(\frac{n}{p}\right)S(1,p)=\left(\frac{n}{p}\right)\tau(\chi).$$

此處

$$\chi(a)=\left(\frac{a}{p}\right).$$

證: 由於

$$x^2\equiv u \pmod p$$

之解數等於

$$1+\left(\frac{u}{p}\right),$$

故

$$\sum_{x=1}^{p} e^{2\pi i x^2 n/p}=\sum_{u=1}^{p}\left(1+\left(\frac{u}{p}\right)\right)e^{2\pi i u n/p}=\sum_{u=1}^{p}\left(\frac{u}{p}\right)e^{2\pi i u n/p}=$$
$$=\left(\frac{n}{p}\right)\sum_{v=1}^{p}\left(\frac{v}{p}\right)e^{2\pi i v/p}.$$

此即定理之結論.

定理 5.

$$S(1,p)=\begin{cases}\sqrt{p}, & \text{若}\ p\equiv 1 \pmod 4,\\ i\sqrt{p}, & \text{若}\ p\equiv 3 \pmod 4.\end{cases}$$

證: 由上定理及定理 4.6, 有

$$S(1,p)=\begin{cases}\pm\sqrt{p}, & \text{若}\ p\equiv 1 \pmod 4,\\ \pm i\sqrt{p}, & \text{若}\ p\equiv 3 \pmod 4,\end{cases}$$

合爲一式,爲

$$\frac{1}{2}(1+i^p)(1-i)S(1,p)=\pm\sqrt{p}.$$

如能證明

$$\Re\left\{\frac{1}{2}(1+i^p)(1-i)S(1,p)\right\}>-\sqrt{p},$$

則定理已明,此處 $\Re x$ 表 x 之實數部分.

易見

$$S(1,p)-1=\sum_{x=1}^{p-1}e^{2\pi i x^2/p}=\sum_{x=1}^{\frac{1}{2}(p-1)}\left(e^{2\pi i x^2/p}+e^{2\pi i(p-x)^2/p}\right)=$$

$$=2\sum_{x=1}^{\frac{1}{2}(p-1)}e^{2\pi i x^2/p}. \tag{1}$$

命 $f(x)$ 爲任一函數,則

$$\sum_{x=1}^{\frac{1}{2}(p-1)}f(x)+\sum_{x=1}^{\frac{1}{2}(p-1)}f\left(\frac{p}{2}-x\right)=\sum_{x=1}^{p-1}f\left(\frac{x}{2}\right).$$

此式顯然眞實,因爲左邊第一項乃右邊 x 等於偶數的各項之和,而第二項乃右邊 x 等於奇數的各項之和.

取 $f(x)=e^{2\pi i x^2/p}$, 並注意 $f\left(\frac{p}{2}-x\right)=i^p e^{2\pi i x^2/p}$. 則由 (1) 可知

$$\frac{1}{2}(1+i^p)(S(1,p)-1)=\sum_{x=1}^{p-1}e^{2\pi i x^2/4p}=W+Z, \tag{2}$$

此處

$$W=\sum_{x\leqslant\sqrt{p}}e^{2\pi i x^2/4p},\qquad Z=\sum_{\sqrt{p}<x\leqslant p-1}e^{2\pi i x^2/4p}. \tag{3}$$

由（2）式，

$$\frac{1}{2}(1+i^p)(1-i)S(1,p)-\frac{1}{2}(1+i^p)(1-i)=(1-i)(W+Z).$$

因爲 $\Re\left\{\frac{1}{2}(1+i^p)(1-i)\right\}=1$ 或 0，故

$$\Re\left\{\frac{1}{2}(1+i^p)(1-i)S(1,p)\right\}\geqslant\Re\{(1-i)(W+Z)\}\geqslant\Re(1-i)W-\sqrt{2}\,|Z|. \quad (4)$$

由於當 $0\leqslant x\leqslant\frac{\pi}{2}$ 時 $\cos x+\sin x\geqslant 1$，故得

$$\Re\{(1-i)W\}=\sum_{x\leqslant\sqrt{p}}\left(\cos\frac{\pi x^2}{2p}+\sin\frac{\pi x^2}{2p}\right)\geqslant[\sqrt{p}\,]\geqslant\frac{1}{2}\sqrt{p}. \quad (5)$$

另一方面，在 Z 中，書

$$v_x=e^{2\pi ix(x+1)/4p},\qquad w_x=\operatorname{cosec}\frac{\pi x}{2p},\qquad q=[\sqrt{p}\,],$$

則

$$(v_x-v_{x-1})w_x=2i\,e^{2\pi ix^2/4p}. \quad (6)$$

故由（3）及（6）可見

$$2iZ=\sum_{x=q+1}^{p-1}(v_x-v_{x-1})w_x,$$

即

$$2|Z|=\left|\sum_{x=q+1}^{p-1}v_x(w_x-w_{x+1})+v_{p-1}w_p-v_q w_{q+1}\right|\leqslant$$

$$\leqslant\sum_{x=q+1}^{p-1}(w_x-w_{x+1})+w_p+w_{q+1}=2w_{q+1}\leqslant$$

$$\leqslant\frac{2p}{q+1}\leqslant 2\sqrt{p} \quad (7)$$

（由於 w_x 之遞減性）．由（4），（5），（7）可知

$$\Re\left\{\frac{1}{2}(1+i^p)(1-i)S(1,p)\right\}\geqslant\left(\frac{1}{2}-\sqrt{2}\right)\sqrt{p}>-\sqrt{p}.$$

故得定理．

總結之，可得以下之結果：

定理 6. 若 m 是奇數，則

$$S(n,m)=\begin{cases}\left(\dfrac{n}{m}\right)\sqrt{m}, & 若\quad m\equiv 1 \pmod 4,\\ i\left(\dfrac{n}{m}\right)\sqrt{m}, & 若\quad m\equiv 3 \pmod 4.\end{cases}$$

證: 於 m 之不同素因子之個數上行歸納法. 當 $m=p^l$ 時由定理 2 及 4 可知

$$S(n,p^l)=\begin{cases}p^{\frac{l}{2}}, & 若\quad 2\mid l,\\ p^{\frac{1}{2}(l-1)}S(n,p)=\left(\dfrac{n}{p}\right)p^{\frac{1}{2}(l-1)}S(1,p)=\end{cases}$$

$$=\begin{cases}\left(\dfrac{n}{p}\right)p^{\frac{l}{2}}, & 若\ 2\nmid l,\quad p\equiv 1 \pmod 4,\\ i\left(\dfrac{n}{p}\right)p^{\frac{l}{2}}, & 若\ 2\nmid l,\quad p\equiv 3 \pmod 4.\end{cases}$$

又由定理 1 及歸納法之假定可知

$$S(n,mm')=S(nm',m)\,S(nm,m')=$$

$$=\left(\frac{nm'}{m}\right)\left(\frac{nm}{m'}\right)i^{\left(\frac{m-1}{2}\right)^2}\sqrt{m}\cdot i^{\left(\frac{m'-1}{2}\right)^2}\sqrt{m'}=$$

$$=\left(\frac{n}{mm'}\right)\left(\frac{m'}{m}\right)\left(\frac{m}{m'}\right)i^{\left(\frac{m-1}{2}\right)^2+\left(\frac{m'-1}{2}\right)^2}\sqrt{mm'}=$$

$$=\left(\frac{n}{mm'}\right)(-1)^{\frac{m-1}{2}\cdot\frac{m'-1}{2}}i^{\left(\frac{m-1}{2}\right)^2+\left(\frac{m'-1}{2}\right)^2}\sqrt{mm'}=$$

$$=\left(\frac{n}{mm'}\right)\sqrt{mm'}\,i^{\left(\frac{m+m'}{2}-1\right)^2}=$$

$$=\begin{cases}\left(\dfrac{n}{mm'}\right)\sqrt{mm'}, & 若\quad mm'\equiv 1 \pmod 4,\\ i\left(\dfrac{n}{mm'}\right)\sqrt{mm'}, & 若\quad mm'\equiv 3 \pmod 4.\end{cases}$$

(此處用了互逆定理.)

定理 7.

$$S(n,2^l)=\begin{cases}0, & 若\ l=1,\\ (1+i^n)\,2^{\frac{l}{2}}, & 若\ l\ 是偶數,\\ 2^{\frac{l+1}{2}}e^{\frac{\pi i}{4}n}, & 若\ l\ 是大于\ 1\ 的奇數.\end{cases}$$

證: 由定理 3, 此結果對 $l=1,2,3$ 已眞實. 對 $l>3$, 則由定理 2 及 3 立得證明。

定理 8. 若 $\chi(n)$ 是實原特徵, mod m, 則

$$\tau(x)=\begin{cases}\sqrt{m}, & 若\ \chi(-1)=1,\\ i\sqrt{m}, & 若\ \chi(-1)=-1.\end{cases}$$

證: 由 §3 已知 m 可書爲

$$m=2^a m',$$

此處 $a=0, 2, 3$, m' 是互不相同的奇素數的乘積;且

1) 若 $a=0$, 則

$$\chi(n)=\left(\frac{n}{m}\right),\qquad (n,m)=1;$$

2) 若 $a=2$, 則

$$\chi(n)=(-1)^{\frac{n-1}{2}}\left(\frac{n}{m'}\right),\qquad (n,m)=1;$$

3) 若 $a=3$, 則

$$\chi(n)=(-1)^{\frac{1}{8}(n^2-1)}\left(\frac{n}{m'}\right)\ 或\ (-1)^{\frac{1}{2}(n-1)+\frac{1}{8}(n^2-1)}\left(\frac{n}{m'}\right),\qquad (n,m)=1.$$

此處 $\left(\frac{n}{m}\right)$ 及 $\left(\frac{n}{m'}\right)$ 是 Jacobi 符號. 今就此三種情況分別討論之.

1) $a=0$. 於 $m=p_1\cdots p_s$ 之素因子之個數上行歸納法. 當 $s=1$ 時, 由定理 5.4 及 5.5 知本定理眞實. 當 $s>1$ 時,命 $m=p_1 m'$, 則由定理 4.1 可知

$$\tau(\chi)=\chi_1(m')\,\chi_2(p_1)\,\tau(\chi_1)\,\tau(\chi_2),$$

此處 χ_1, χ_2 分別以 p_1, m' 爲模, 且 $\chi(n)=\chi_1(n)\,\chi_2(n)$. 於是由定理 3.6.4 及歸納法之假設得

$$\tau(\chi)=\left(\frac{m'}{p_1}\right)\left(\frac{p_1}{m'}\right)\cdot\begin{Bmatrix}\sqrt{p_1}\\ i\sqrt{p_1}\end{Bmatrix}\cdot\begin{Bmatrix}\sqrt{m'}\\ i\sqrt{m'}\end{Bmatrix}=$$

$$=(-1)^{\frac{p_1-1}{2}\cdot\frac{m'-1}{2}}\cdot\begin{Bmatrix}\sqrt{p_1}\\ i\sqrt{p_1}\end{Bmatrix}\cdot\begin{Bmatrix}\sqrt{m'}\\ i\sqrt{m'}\end{Bmatrix}=$$

$$=\begin{cases}\sqrt{p_1m'}=\sqrt{m}, & 若\ m\equiv 1\pmod 4\ 或\ \chi(-1)=1,\\ i\sqrt{p_1m'}=i\sqrt{m}, & 若\ m\equiv 3\pmod 4\ 或\ \chi(-1)=-1.\end{cases}$$

2) $a=2$, 即 $m=2^2m'$. 若 $m'=1$, 則 $\chi(1)=1$, $\chi(3)=-1$, 於是

$$\tau(\chi)=\sum_{n=1}^{4}\chi(n)\,e^{2\pi in/4}=e^{2\pi i/4}-e^{6\pi i/4}=2i.$$

若 $m'>1$, 則由定理 4.1 及 1)

$$\tau(\chi)=(-1)^{\frac{m'-1}{2}}\left(\frac{4}{m'}\right)2i\cdot\begin{cases}\sqrt{m'}=i\sqrt{m}, & \text{若 } m'\equiv 1 \pmod 4 \text{ 或 } \chi(-1)=-1,\\ i\sqrt{m'}=\sqrt{m}, & \text{若 } m'\equiv 3 \pmod 4 \text{ 或 } \chi(-1)=1.\end{cases}$$

3) $a=3$, 即 $m=2^3m'$. 當 $m'=1$ 時,有

$$\tau(\chi)=\sum_{n=1}^{8}\chi(n)\,e^{2\pi in/8}=\begin{cases}e^{2\pi i/8}-e^{6\pi i/8}-e^{10\pi i/8}+e^{14\pi i/8}=\sqrt{8}, & \text{若 } \chi(-1)=1,\\ e^{2\pi i/8}+e^{6\pi i/8}-e^{10\pi i/8}-e^{14\pi i/8}=i\sqrt{8}, & \text{若 } \chi(-1)=-1.\end{cases}$$

當 $m'>1$ 時, 若 $\chi(n)=(-1)^{\frac{1}{8}(n^2-1)}\left(\frac{n}{m'}\right)$, 則

$$\tau(\chi)=(-1)^{\frac{1}{8}(m'^2-1)}\left(\frac{8}{m'}\right)\sqrt{8}\cdot\begin{cases}\sqrt{m'}=\sqrt{m}, & \text{若 } m'\equiv 1 \pmod 4 \text{ 或 } \chi(-1)=1,\\ i\sqrt{m'}=i\sqrt{m}, & \text{若 } m'\equiv 3 \pmod 4 \text{ 或 } \chi(-1)=-1.\end{cases}$$

若 $\chi(n)=(-1)^{\frac{1}{2}(n-1)+\frac{1}{8}(n^2-1)}\left(\frac{n}{m'}\right)$, 則

$$\tau(\chi)=(-1)^{\frac{1}{2}(m'-1)+\frac{1}{8}(m'^2-1)}\left(\frac{8}{m'}\right)i\sqrt{8}\cdot$$

$$\cdot\begin{cases}\sqrt{m'}=i\sqrt{m}, & \text{若 } m'\equiv 1 \pmod 4 \text{ 或 } \chi(-1)=-1,\\ i\sqrt{m'}=\sqrt{m}, & \text{若 } m'\equiv 3 \pmod 4 \text{ 或 } \chi(-1)=1.\end{cases}$$

合 1),2),3) 即得定理。

§6. 特徵和與三角和.

由上節已知 Gauss 和與特徵和之關係. 今更進一步建立某些三角和與特徵和之關係.

定理 1. 設 p 為一素數, $d\mid p-1$. 一整數 x 為 d 次非剩餘, mod p, 之必要且充分條件為

$$\frac{1}{d}\sum_{a=1}^{d}e^{2\pi i a\,\mathrm{ind}\,x/d}=0;$$

不然,則此式等於 1.

證: 由定理 3.8.1, x 是 d次剩餘與否視 $d\mid\mathrm{ind}\,x$ 或 $d\nmid\mathrm{ind}\,x$ 而定 用

三角和,此卽表示

$$\frac{1}{d}\sum_{a=1}^{d} e^{2\pi i a \operatorname{ind} x/d}=\begin{cases}1, & \text{若 } x \text{ 是 } d \text{ 次剩餘, mod } p,\\ 0, & \text{若 } x \text{ 是 } d \text{ 次非剩餘, mod } p.\end{cases}$$

定理 2. 命 p 爲一素數, $p \nmid a$, $(p-1, k)=d$, 則

$$\sum_{x=1}^{p} e^{2\pi i a x^k/p}=\sum_{b=1}^{d-1} S(a, \chi^b),$$

此處

$$\chi(u)=e^{2\pi i \operatorname{ind} u/d}.$$

證: 因 $x^k \equiv u \pmod p$ 或無根,或有 $d=(p-1, k)$ 個根,故由定理 1 得

$$\sum_{x=1}^{p} e^{2\pi i a x^k/p}=1+\sum_{u=1}^{p-1} e^{2\pi i a u/p} \sum_{b=1}^{d} e^{2\pi i b \operatorname{ind} u/d}=$$

$$=1+\sum_{b=1}^{d} \sum_{u=1}^{p-1} e^{2\pi i a u/p} \chi^b(u)=$$

$$=1+\sum_{u=1}^{p-1} e^{2\pi i a u/p}+\sum_{b=1}^{d-1} \sum_{u=1}^{p-1} e^{2\pi i a u/p} \chi^b(u)=$$

$$=\sum_{b=1}^{d-1} S(a, \chi^b).$$

由定理 4.3 及 4.5 已知 $|S(a, \chi^b)| \leqslant \sqrt{p}$, 故得:

定理 3. 命 $d=(k, p-1)$,則

$$\left|\sum_{x=1}^{p} e^{2\pi i a x^k/p}\right| \leqslant (d-1) \sqrt{p}.$$

習題. 仿定理 5.1 及 5.2 以研究三角和

$$\sum_{x=0}^{m-1} e^{2\pi i x^k n/m}, \quad (n, m)=1.$$

§ 7. 由完整和到不完整和.

定理 1. $g(x)$ 表一週期爲 q 的函數,且

$$g(x)=\begin{cases}1, & \text{當 } 0 \leqslant x<m,\\ 0, & \text{當 } m \leqslant x<q.\end{cases}$$

則 $g(x)$ 可表爲

$$g(x)=\frac{m}{q}+\frac{1}{q}\sum_{n=1}^{q-1}e^{2\pi inx/q}\left(1-e^{-2\pi inm/q}\right)/\left(1-e^{-2\pi in/q}\right).$$

證：顯然

$$g(x)=\frac{1}{q}\sum_{n=0}^{q-1}e^{2\pi inx/q}\sum_{t=0}^{m-1}e^{-2\pi int/q}$$

$$=\frac{m}{q}+\frac{1}{q}\sum_{n=1}^{q-1}e^{2\pi inx/q}\,\frac{1-e^{-2\pi inm/q}}{1-e^{-2\pi in/q}}.$$

定理 2. 命 α 爲實數及

$$S=\sum_{q'<n\leqslant q''}e^{2\pi in\alpha},$$

則

$$|S|\leqslant\min\left(q''-q',\ \frac{1}{2\langle\alpha\rangle}\right),$$

此處 $\langle\alpha\rangle=\min\left(\alpha-[\alpha],\ [\alpha]+1-\alpha\right)$.

證：顯然有不等式

$$|S|\leqslant q''-q'.$$

若 $\alpha\neq[\alpha]$，命 $Q=q''-q'$，則有

$$|S|=\left|\sum_{n=0}^{Q-1}e^{2\pi in\alpha}\right|=\left|\frac{1-e^{2\pi iQ\alpha}}{1-e^{2\pi i\alpha}}\right|\leqslant$$

$$\leqslant\frac{2}{|1-e^{2\pi i\alpha}|}=\frac{1}{|\sin\pi\alpha|}\leqslant$$

$$\leqslant\frac{1}{2\langle\alpha\rangle}$$

$\left(\text{當 } 0\leqslant\xi\leqslant\frac{1}{2}\text{ 時, }\sin\pi\xi\geqslant2\xi\text{, 所以有 }|\sin\pi\xi|\geqslant2\langle\xi\rangle\right).$

定理 3. 若 $2\nmid q$，則

$$\left|\sum_{x=0}^{m-1}e^{2\pi ix^2/q}-\frac{m}{q}\sum_{x=0}^{q-1}e^{2\pi ix^2/q}\right|\leqslant\sqrt{q}\log q.$$

證：顯然可以假定 $m\leqslant q$. 由定理 1 可知

$$\sum_{x=0}^{m-1}e^{2\pi ix^2/q}=\sum_{x=0}^{q-1}e^{2\pi ix^2/q}g(x)=$$

$$=\frac{m}{q}\sum_{x=0}^{q-1}e^{2\pi ix^2/q}+\frac{1}{q}\sum_{n=1}^{q-1}\sum_{x=0}^{q-1}e^{2\pi i(x^2+nx)/q}\,\frac{1-e^{-2\pi inm/q}}{1-e^{-2\pi in/q}}.$$

由 Gauss 和之公式可知

$$\left|\sum_{x=0}^{q-1} e^{2\pi i(x^2+nx)/q}\right| = \left|\sum_{x=0}^{q-1} e^{2\pi i(x+\frac{1}{2}n)^2/q}\right|^{*)} \leqslant \sqrt{q},$$

故得

$$\left|\sum_{x=0}^{q-1} e^{2\pi i x^2/q} - \frac{m}{q}\sum_{x=0}^{q-1} e^{2\pi i x^2/q}\right| \leqslant \frac{1}{\sqrt{q}}\sum_{n=1}^{q-1}\frac{1}{2\left\langle\frac{n}{q}\right\rangle} \leqslant$$

$$\leqslant \frac{1}{\sqrt{q}}\sum_{n=1}^{\frac{1}{2}(q-1)}\frac{q}{n} = \sqrt{q}\sum_{n=1}^{\frac{1}{2}(q-1)}\frac{1}{n} <$$

$$< \sqrt{q}\sum_{n=1}^{\frac{1}{2}(q-1)}\left(-\log\left(1-\frac{1}{2n}\right)+\log\left(1+\frac{1}{2n}\right)\right)=$$

$$= \sqrt{q}\sum_{n=1}^{\frac{1}{2}(q-1)}(-\log(2n-1)+\log(2n+1))=$$

$$= \sqrt{q}\log q.$$

定理 4 (Pólya). 命 p 爲一奇素數, $1 \leqslant m \leqslant p$, χ 非主特徵, mod p, 則

$$\left|\sum_{x=0}^{m-1}\chi(x)\right| < \sqrt{p}\log p.$$

證: 由定理 1 可知

$$\sum_{x=0}^{m-1}\chi(x) = \sum_{x=0}^{p-1}\chi(x)\,g(x)=$$

$$= \frac{m}{p}\sum_{x=0}^{p-1}\chi(x) + \frac{1}{p}\sum_{x=0}^{p-1}\chi(x)\sum_{n=1}^{p-1} e^{2\pi i nx/p}\frac{1-e^{-2\pi i nm/p}}{1-e^{-2\pi i n/p}}.$$

由定理 2.3, 定理 4.5 及定理 2 可知

$$\left|\sum_{x=0}^{m-1}\chi(x)\right| \leqslant \frac{1}{p}\sum_{n=1}^{p-1}\left|\frac{1-e^{-2\pi i nm/p}}{1-e^{-2\pi i n/p}}\right|\left|\sum_{x=0}^{p-1}\chi(x)\,e^{2\pi i nx/p}\right| \leqslant$$

$$\leqslant \frac{1}{\sqrt{p}}\sum_{n=1}^{p-1}\frac{1}{2\left\langle\frac{n}{p}\right\rangle} < \sqrt{p}\log p.$$

---

*) 此處之 $\frac{1}{2}$ 乃表示同餘式

$$2x \equiv 1 \pmod q$$

之解, 以下準此.

此定理有以下之應用:

定理 5. 命 p 爲奇素數, $d|(p-1)$, 則對模 p 必有一小於 $\sqrt{p}\log p$ 之 d 次非剩餘.

證: 命 R 表不大於 m 之 d 次剩餘數,則

$$R=\sum_{x=1}^{m}\frac{1}{d}\sum_{a=1}^{d}e^{2\pi ia\operatorname{ind}x/d}=\frac{1}{d}\sum_{a=1}^{d}\sum_{x=1}^{m}e^{2\pi ia\operatorname{ind}x/d}=$$

$$=\frac{m}{d}+\frac{1}{d}\sum_{a=1}^{d-1}\sum_{x=1}^{m}(\chi(x))^{a},$$

此處 $\chi(x)=e^{2\pi i\operatorname{ind}x/d}$. 由定理 4 可知

$$\left|R-\frac{m}{d}\right|<\frac{d-1}{d}\sqrt{p}\log p. \tag{1}$$

即

$$R<\frac{m}{d}+\frac{d-1}{d}\sqrt{p}\log p.$$

當 $m=\sqrt{p}\log p$ 時,

$$R<\frac{m}{d}+\frac{d-1}{d}m=m,$$

故有小於 $\sqrt{p}\log p$ 的 d 次非剩餘存在.

特別必有二次非剩餘 $<\sqrt{p}\log p$. 求最小之方次 δ 使最小二次非剩餘$=O(p^{\delta})$ 是一有名難題. Виноградов 之結果爲

定理 6. 若 p 充分大, 則關於模 p 之最小二次非剩餘 $\leqslant p^{\frac{1}{2\sqrt{e}}}(\log p)^2$ $\left(=O\left(p^{\frac{1}{3.2}}\right)\right)$.

證: 命

$$T=[p^{\frac{1}{2\sqrt{e}}}(\log p)^2],\qquad m=\sqrt{p}(\log p)^2.$$

設 $1,2,\cdots,T$ 皆爲二次剩餘. 因每一二次非剩餘必有一素因子亦爲二次非剩餘, 故每一不大於 m 之二次非剩餘必有一素因子 q, 使 $T<q\leqslant m$. 故如命 N 表不大於 m 之二次非剩餘數,則有

$$N\leqslant\sum_{T<q\leqslant m}\left[\frac{m}{q}\right]<m\sum_{T<q\leqslant m}\frac{1}{q}.$$

由定理 5.9.2,

$$N < m \log \frac{\log m}{\log T} + O\left(\frac{m}{\log T}\right) =$$

$$= m\left(\frac{1}{2} + \log \frac{1 + \dfrac{4 \log \log p}{\log p}}{1 + \dfrac{4\sqrt{e} \log \log p}{\log p}}\right) + O\left(\frac{m}{\log T}\right) =$$

$$= m\left(\frac{1}{2} - \frac{4(\sqrt{e}-1) \log \log p}{\log p}\right) + O\left(\frac{m}{\log T}\right).$$

由 (1) 可知 $N = \frac{m}{2} + O(\sqrt{p} \log p) = \frac{m}{2} + O\left(\frac{m}{\log p}\right)$, 故得

$$\frac{m}{2} + O\left(\frac{m}{\log p}\right) < m\left(\frac{1}{2} - \frac{4(\sqrt{e}-1) \log \log p}{\log p}\right) + O\left(\frac{m}{\log p}\right),$$

即

$$\log \log p = O(1),$$

當 p 充分大時,此爲不可能. 故定理得證.

§ 8. 特徵和 $\sum_{x=1}^{p}\left(\frac{x^2+ax+b}{p}\right)$ 之應用舉例.

定 理 1. 共有

$$\frac{1}{4}\left(p - 4 - \left(\frac{-1}{p}\right)\right)$$

個數 a, 使 a 及 $a+1$ 皆爲二次剩餘, mod p.

在證明此定理之前,先得算出一和之值.

定 理 2. 設 $p > 2$, $a^2 - 4b \not\equiv 0 \pmod p$,則

$$\sum_{x=1}^{p}\left(\frac{x^2+ax+b}{p}\right) = -1.$$

式中遇及 $p | x^2 + ax + b$ 之項,則該項以 0 代之.

證: 可假定 $a = 0$, 若不然則以 $y = x + \frac{1}{2}a$ 代之.

今設 $a = 0$, $p \nmid b$. 由 Euler 判別定理,

$$\sum_{x=1}^{p}\left(\frac{x^2+b}{p}\right) \equiv \sum_{x=1}^{p} (x^2+b)^{\frac{1}{2}(p-1)} \pmod p. \tag{1}$$

命 g 爲 p 之原根. 若 $0 < c < p-1$, 則

$$\sum_{x=1}^{p} x^c \equiv \sum_{v=0}^{p-2} g^{cv} = \frac{1-g^{c(p-1)}}{1-g^c} \equiv 0 \pmod p.$$

以此代入 (1) 式,卽得

$$\sum_{x=1}^{p}\left(\frac{x^2+b}{p}\right) \equiv \sum_{x=1}^{p} x^{p-1} \equiv \sum_{x=1}^{p-1} 1 \equiv$$
$$\equiv -1 \pmod p.$$

顯然

$$\left|\sum_{x=1}^{p}\left(\frac{x^2+b}{p}\right)\right| \leqslant p,$$

故

$$\sum_{x=1}^{p}\left(\frac{x^2+b}{p}\right) = -1 \text{ 或 } p-1.$$

又因爲

$$\sum_{x=1}^{p}\left(\frac{x^2+b}{p}\right) = \left(\frac{b}{p}\right) + 2\sum_{x=1}^{\frac{1}{2}(p-1)}\left(\frac{x^2+b}{p}\right) \equiv$$
$$\equiv 1 \pmod 2,$$

故

$$\sum_{x=1}^{p}\left(\frac{x^2+b}{p}\right) = -1.$$

定理 1 之證明: 具有定理中之性質之 a 之個數可以表爲

$$\frac{1}{4}\sum_{a=1}^{p-2}\left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{a+1}{p}\right)\right) =$$
$$= \frac{1}{4}\sum_{a=1}^{p-2}\left(1+\left(\frac{a}{p}\right)+\left(\frac{a+1}{p}\right)+\left(\frac{a(a+1)}{p}\right)\right) =$$
$$= \frac{1}{4}\left(p-2-\left(\frac{-1}{p}\right)-\left(\frac{1}{p}\right)-1\right) =$$
$$= \frac{1}{4}\left(p-4-\left(\frac{-1}{p}\right)\right)$$

(因 $\sum_{a=1}^{p}\left(\frac{a}{p}\right) = 0$).

由定理 1 立得:

定理 3. 若 $p \geqslant 7$, 則必有二連續之數皆爲二次剩餘.

同法可證:

定理 4. 共有 $\frac{1}{4}\left(p-2+\left(\frac{-1}{p}\right)\right)$ 個數 a, 使 a 及 $a+1$ 皆爲二次非剩餘. 故若 $p\geqslant 5$, 必有二連續之數皆爲二次非剩餘.

定理 5. 共有 $\frac{1}{2}(p-1)$ 個 a, 使 a 及 $a+1$ 不同時爲二次剩餘或二次非剩餘.

證: 由 $\sum_{a=1}^{p-2}\left(1-\left(\frac{a}{p}\right)\left(\frac{a+1}{p}\right)\right)=p-1$ 立得定理.

附記: 若問及連續三數同爲二次剩餘,則必須研究特徵和

$$\sum_{x=1}^{p}\left(\frac{x(x+1)(x+2)}{p}\right).$$

此乃一超出本書範圍之問題. 但對三次多項式之特徵和有次之應用.

定理 6 (Горшков). 命 p 爲一素數 $\equiv 1 \pmod 4$, 則

$$p=x^2+y^2$$

之整數解可以表成爲 $x=\frac{1}{2}S(r), y=\frac{1}{2}S(u)$, 此處 $\left(\frac{r}{p}\right)=1, \left(\frac{u}{p}\right)=-1$, 且

$$S(k)=\sum_{x=1}^{p-1}\left(\frac{x(x^2+k)}{p}\right).$$

證: 由於

$$S(k)=\sum_{x=1}^{\frac{1}{2}(p-1)}\left(\frac{x(x^2+k)}{p}\right)+\sum_{y=1}^{\frac{1}{2}(p-1)}\left(\frac{(p-y)((p-y)^2+k)}{p}\right)=$$

$$=2\sum_{x=1}^{\frac{1}{2}(p-1)}\left(\frac{x(x^2+k)}{p}\right),$$

故 x 及 y 是整數. 又當 $p\nmid t$ 時,

$$\left(\frac{t}{p}\right)^3 S(k)=\sum_{x=1}^{p-1}\left(\frac{tx((tx)^2+t^2k)}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{x(x^2+t^2k)}{p}\right)=S(t^2k).$$

今討論

$$\frac{p-1}{2}((S(r))^2+(S(u))^2)=\sum_{t=1}^{\frac{1}{2}(p-1)}(S(rt^2))^2+\sum_{t=1}^{\frac{1}{2}(p-1)}(S(ut^2))^2=$$

$$=\sum_{k=1}^{p-1}(S(k))^2=\sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\sum_{k=1}^{p-1}\left(\frac{xy(x^2+k)(y^2+k)}{p}\right).$$

由定理 2 可知上式之內和

$$=\begin{cases}-2\left(\frac{xy}{p}\right), & 若\ x\not\equiv\pm y\ (\mathrm{mod}\ p),\\ p-2, & 若\ x\equiv\pm y\ (\mathrm{mod}\ p).\end{cases}$$

故

$$\sum_{k=1}^{p-1}(S(k))^2=2(p-1)(p-2)-2\sum\sum_{\substack{x\not\equiv\pm y\\(\mathrm{mod}\ p)}}\left(\frac{xy}{p}\right)=$$

$$=2p(p-1)-2\sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\left(\frac{xy}{p}\right)=2p(p-1).$$

總之,得出

$$(S(r))^2+(S(u))^2=4p.$$

§9. 原根之分佈問題.

定理 1. 命 p 爲一奇素數及 $p\nmid n$. 若 n 非原根, mod p, 則

$$\sum_{k\mid p-1}\frac{\mu(k)}{\varphi(k)}\sum_{\substack{a=1\\(a,k)=1}}^{k}e^{2\pi ia\,\mathrm{ind}\,n/k}=0. \tag{1}$$

證: 由於

$$\sum_{\substack{a=1\\(a,k)=1}}^{k}e^{2\pi ia\,\mathrm{ind}\,n/k}$$

爲 k 之積性函數,及 $\mu(k)$ 與 $\varphi(k)$ 也是積性函數,故 (1) 式之左邊等於

$$\prod_{q\mid p-1}\left(1+\frac{\mu(q)}{\varphi(q)}\sum_{\substack{a=1\\(a,q)=1}}^{q}e^{2\pi ia\,\mathrm{ind}\,n/q}\right),$$

此處 q 過 $p-1$ 不同的素因子.

若 n 非原根, 則有 $(\mathrm{ind}\ n,\ p-1)>1$, 卽有一 $p-1$ 之素因子 q 整除 ind n. 而對這一素數

$$1+\frac{\mu(q)}{\varphi(q)}\sum_{\substack{a=1\\(a,q)=1}}^{q}e^{2\pi ia\,\mathrm{ind}\,n/q}=$$

$$=1+\frac{-1}{q-1}\cdot(q-1)=0.$$

故得定理.

定理 2. 命 p 爲一奇素數，$1 \leqslant A < p$. 若 $\chi(n)$ 非主特徵，mod p，則

$$\frac{1}{A+1}\left|\sum_{a=0}^{A}\sum_{n=-a}^{a}\chi(n)\right| \leqslant p^{\frac{1}{2}} - \frac{A+1}{p^{\frac{1}{2}}}. \tag{2}$$

證：已知

$$|\tau(\chi)| = \left|\sum_{h=1}^{p-1}\chi(h)\,e^{2\pi ih/p}\right| = p^{\frac{1}{2}}.$$

若 $p \nmid n$，則

$$\chi(n)\,\tau(\bar{\chi}) = \chi(n)\sum_{h=1}^{p-1}\bar{\chi}(h)\,e^{2\pi ih/p} =$$

$$= \chi(n)\sum_{h=1}^{p-1}\bar{\chi}(nh)\,e^{2\pi inh/p} =$$

$$= \sum_{h=1}^{p-1}\bar{\chi}(h)\,e^{2\pi inh/p}.$$

(2) 式左邊乘以 $\tau(\bar{\chi})$，則得

$$\frac{\sqrt{p}}{A+1}\left|\sum_{a=0}^{A}\sum_{n=-a}^{a}\chi(n)\right| = \frac{1}{A+1}\left|\sum_{a=0}^{A}\sum_{n=-a}^{a}\chi(n)\,\tau(\bar{\chi})\right| =$$

$$= \frac{1}{A+1}\left|\sum_{a=0}^{A}\sum_{n=-a}^{a}\sum_{h=1}^{p-1}\bar{\chi}(h)\,e^{2\pi inh/p}\right| =$$

$$= \frac{1}{A+1}\left|\sum_{h=1}^{p-1}\bar{\chi}(h)\left(\frac{\sin\,(A+1)\,\pi h/p}{\sin\,\pi h/p}\right)^2\right|, \tag{3}$$

此處用了公式

$$\sum_{a=0}^{A}\sum_{n=-a}^{a}e^{2\pi inh/p} = \left(\frac{\sin\,(A+1)\,\pi h/p}{\sin\,\pi h/p}\right)^2, \tag{4}$$

此式不難直接算出.

由 (3) 及 (4) 即得

$$\frac{\sqrt{p}}{A+1}\left|\sum_{a=0}^{A}\sum_{n=-a}^{a}\chi(n)\right| \leqslant \frac{1}{A+1}\sum_{h=1}^{p-1}\left(\frac{\sin\,(A+1)\,\pi h/p}{\sin\,\pi h/p}\right)^2 =$$

$$= \frac{1}{A+1}\sum_{h=1}^{p-1}\sum_{a=0}^{A}\sum_{n=-a}^{a}e^{2\pi inh/p} =$$

$$= \frac{1}{A+1}\sum_{a=0}^{A}\sum_{n=-a}^{a}\left(\sum_{h=1}^{p}e^{2\pi inh/p} - 1\right) =$$

$$=p-(A+1).$$

定理 3. 命 $h(p)$ 代表絕對值最小的原根，mod p. 則

$$|h(p)|<2^m p^{\frac{1}{2}},$$

此處 m 乃 $p-1$ 之不同素因子之個數.

證：命 $p>2$. 由定理 1，可知

$$0=\sum_{k\mid p-1}\frac{\mu(k)}{\varphi(k)}\sum_{\substack{u=1\\(u,k)=1}}^{k}\sum_{a=0}^{|h(p)|-1}\sum_{n=-a}^{a}{}' e^{2\pi iu\,\mathrm{ind}\,n/k},$$

此處 Σ' 表示除去 $n=0$ 的一項. 此式之右邊當 $k=1$ 之一項等於

$$\sum_{a=0}^{|h(p)|-1}\sum_{n=-a}^{a}{}'1=\sum_{a=0}^{|h(p)|-1}2a=|h(p)|^2-|h(p)|.$$

對於 $k\neq 1$ 之各項用定理 2，取 $A=|h(p)|-1$，則

$$\left|\sum_{a=0}^{|h(p)|-1}\sum_{n=-a}^{a}{}'\chi(n)\right|\leqslant |h(p)|\,p^{\frac{1}{2}}-\frac{|h(p)|^2}{p^{\frac{1}{2}}},$$

此處

$$\chi(n)=e^{2\pi iu\,\mathrm{ind}\,n/k}.$$

故得

$$|h(p)|^2-|h(p)|\leqslant\left(|h(p)|\,p^{\frac{1}{2}}-\frac{|h(p)|^2}{p^{\frac{1}{2}}}\right)\sum_{k\mid p-1}\frac{|\mu(k)|}{\varphi(k)}\varphi(k)=$$

$$=2^m\left(|h(p)|\,p^{\frac{1}{2}}-\frac{|h(p)|^2}{p^{\frac{1}{2}}}\right).$$

即

$$|h(p)|\leqslant\frac{2^m p^{\frac{1}{2}}+1}{1+2^m/p^{\frac{1}{2}}}<2^m p^{\frac{1}{2}}.$$

由定理 3 立刻可推得：

定理 4. 若 $p\equiv 1 \pmod 4$，則原根

$$g(p)=|h(p)|<2^m p^{\frac{1}{2}}.$$

證：今須證明 $|h(p)|$ 是一原根. 假定不然，則 $-|h(p)|$ 爲一原根. 但

$$|h(p)|^l\equiv 1 \pmod p,\qquad l<p-1.$$

故

$$(h(p))^{2l}\equiv 1 \pmod p.$$

由於 $-|h(p)|$ 是原根,可知 $2l=p-1$. 故

$$|h(p)|^{\frac{p-1}{2}}\equiv 1 \pmod p.$$

卽 $|h(p)|$ 爲二次剩餘. 因 -1 也是二次剩餘, 故 $-|h(p)|$ 也是二次剩餘. 此與 $-|h(p)|$ 是原根的假定相違背.

定理 5. 模 p 之最小正原根 $g(p)$ 適合於

$$g(p)<2^{m+1}p^{\frac{1}{2}}.$$

證: 取 $A=[(g(p)-1)/2]$, 則

$$0=\sum_{k|p-1}\frac{\mu(k)}{\varphi(k)}\sum_{\substack{u=1\\(u,k)=1}}^{k}\sum_{a=0}^{A}\sum_{n=A+1-a}^{A+1+a}e^{2\pi iu\operatorname{ind}n/k},$$

上式右邊 $k=1$ 之一項等於

$$\sum_{a=0}^{A}\sum_{n=A+1-a}^{A+1+a}1=\sum_{a=0}^{A}(2a+1)=(A+1)^2;$$

其 $k\neq 1$ 之項,如定理 2 可以證明

$$\left|\sum_{a=0}^{A}\sum_{n=A+1-a}^{A+1+a}e^{2\pi iu\operatorname{ind}n/k}\right|\leqslant(A+1)p^{\frac{1}{2}}-\frac{1}{p^{\frac{1}{2}}}(A+1)^2.$$

故如定理 4 可得

$$(A+1)^2\leqslant 2^m\left((A+1)p^{\frac{1}{2}}-\frac{1}{p^{\frac{1}{2}}}(A+1)^2\right),$$

$$\frac{1}{2}(g(p)-1)<A+1\leqslant\frac{2^m p^{\frac{1}{2}}}{1+2^m/p^{\frac{1}{2}}},$$

卽

$$g(p)\leqslant\frac{2^{m+1}p^{\frac{1}{2}}}{1+2^m/p^{\frac{1}{2}}}+1<2^{m+1}p^{\frac{1}{2}}.$$

§ 10. 含多項式之三角和.

本節之主要目的在證明:

定理 1. 命 $f(x)$ 表一整係數多項式

$$f(x)=a_k x^k+\cdots+a_1x+a_0.$$

若 $(a_k,\cdots,a_0,q)=1$, 則

$$S(q,f(x))=\sum_{x=1}^{q}e^{2\pi i f(x)/q}=O(q^{1-\frac{1}{k}+\varepsilon}),$$

此處 ε 爲任與之正數，O 中所包含之常數僅與 k 及 ε 有關.

因爲

$$|e^{2\pi i a_0/q}|=1,$$

故常可假定 $f(0)=0$，而不失其普遍性. 今分幾個步驟來證明本定理.

定理 2. 若 $(q_1, q_2)=1$，則

$$S(q_1 q_2, f(x))=S(q_1, f(q_2 x)/q_2)\,S(q_2, f(q_1 x)/q_1).$$

證：命 $x=q_1 y+q_2 z$，當 y 及 z 各過以 q_2 及 q_1 爲模之完全剩餘系時，x 過以 $q_1 q_2$ 爲模之完全剩餘系. 顯然有

$$e^{2\pi i f(q_1 y+q_2 z)/q_1 q_2}=e^{2\pi i f(q_1 y)/q_1 q_2}\cdot e^{2\pi i f(q_2 z)/q_1 q_2},$$

故

$$S(q_1 q_2, f(x))=\sum_{x=1}^{q_1 q_2}e^{2\pi i f(x)/q_1 q_2}=$$

$$=\sum_{y=1}^{q_2}\sum_{z=1}^{q_1}e^{2\pi i f(q_1 y)/q_1 q_2}\cdot e^{2\pi i f(q_2 z)/q_1 q_2}=$$

$$=S(q_1, f(q_2 x)/q_2)\,S(q_2, f(q_1 x)/q_1).$$

由此定理可知主要在研究 $q=p^l$ 之情況.

引 1. 設 $f(x)$ 是一整係數多項式，mod p, α 是

$$f(x)\equiv 0 \pmod p$$

之 m 重根. $p^u \| f(px+\alpha)$*). 命 $g(x)=p^{-u}f(px+\alpha)$，則

$$g(x)\equiv 0 \pmod p$$

至多有 m 個根.

證：並不失其普遍性，可以假定 $\alpha=0$. 如是則

$$f(x)=x^m f_1(x)+p\,f_2(x),$$

此處 $f_1(0)\not\equiv 0 \pmod p$，$f_2(x)$ 之次數 $<m$. $f_1(x)$ 及 $f_2(x)$ 都是整係數多項

*) 我們用符號 $p^u \| a$ 表示 $p^u | a$ 而 $p^{u+1}\nmid a$. 用 $p^u \| S(x)$ 表示 p^u 整除 $S(x)$ 之所有係數，而 p^{u+1} 則否.

式. 由是得

$$f(px) = p^m x^m f_1(px) + p f_2(px).$$

因 p^{m+1} 除不盡 x^m 之係數 $p^m f_1(0)$, 故 $u \leqslant m$. 又因 $p^{-u}f(px)$ 之次數 $\leqslant m$ $(\bmod p)$,故得本引理。

引 2. 設 $f(x) = a_k x^k + \cdots + a_1 x$ 是整係數多項式, $p \nmid (a_k, \cdots, a_1)$, $p^t \| (ka_k, \cdots, 2a_2, a_1)$. 設 μ 爲

$$f'(x) \equiv 0 \pmod{p^{t+1}}, \qquad 0 \leqslant x < p$$

之一根. 又設 $p^\sigma \| (f(\mu + px) - f(\mu))$,則

$$1 \leqslant \sigma \leqslant k.$$

證: 設 $\sigma \geqslant k+1$, 則由假定

$$p^\sigma \left| \frac{p^h}{h!} f^{(h)}(\mu), \qquad 1 \leqslant h \leqslant k. \right.$$

卽對任一 h $(1 \leqslant h \leqslant k)$ 常有

$$p^{k+1} \left| \frac{p^h}{h!} f^{(h)}(\mu), \right.$$

由此得出

$$p \left| \frac{1}{h!} f^{(h)}(\mu). \right.$$

因而得出 $p|a_k, p|a_{k-1}, \cdots, p|a_1$. 此與假定 $p \nmid (a_k, \cdots, a_1)$ 相違背.

基本引理. 若 $p \nmid (a_k, \cdots, a_1)$,則

$$|S(p^l, f(x))| < C(k)\, p^{l\left(1-\frac{1}{k}\right)}.$$

證: 我們用歸納法來證明本引理.

今先證明 $l = 1$ 之情況. 顯然我們可以假定 $p > k$.

命 N 表示同餘方程組

$$x_1^h + \cdots + x_k^h \equiv y_1^h + \cdots + y_k^h \pmod p, \quad 1 \leqslant x, y \leqslant p, \quad h = 1, 2, \cdots, k \tag{1}$$

之解答數. 簡書 $\sum_{x=1}^{p}$ 爲 $\sum_x$, $e^{2\pi i f(x)/p}$ 爲 $e_p(f(x))$, 則由定理 1.1 可得

$$\sum_{a_k} \cdots \sum_{a_1} \left| \sum_x e_p(a_k x^k + \cdots + a_1 x) \right|^{2k} =$$

$$= \sum_{x_1} \cdots \sum_{x_k} \sum_{y_1} \cdots \sum_{y_k} \sum_{a_k} \cdots \sum_{a_1} e_p\left(a_k(x_1^k + \cdots + x_k^k - y_1^k - \cdots - y_k^k) + \cdots + \right.$$

$$\left. + a_1(x_1 + \cdots + x_k - y_1 - \cdots - y_k)\right) = p^k N.$$

利用對稱函數中習知的定理，由 (1) 可得

$$(x-x_1)\cdots(x-x_k) \equiv (x-y_1)\cdots(x-y_k) \pmod p.$$

故 $x_1, \cdots, x_k$ 與 $y_1, \cdots, y_k$ 實僅有次序之差異，mod p. 所以

$$N \leqslant k!\, p^k.$$

卽

$$\sum_{a_k} \cdots \sum_{a_1} \left| \sum_x e_p(a_k x^k + \cdots + a_1 x) \right|^{2k} \leqslant k!\, p^{2k}. \tag{2}$$

對於任一 λ ($\not\equiv 0 \pmod p$) 及任一 μ，顯然有

$$|S(p, f(x))| = |S(p, f(\lambda x+\mu) - f(\mu))|.$$

所有這種形式的和皆在 (2) 之左邊出現. 今將係數各各同餘，mod p，之二多項式算爲全同，mod p. 我們來求多項式 $f(\lambda x + \mu) - f(\mu)$ ($\lambda = 1, \cdots, p-1$, $\mu = 0, 1, \cdots, p-1$) 中互不相同之多項式的數目. 不失其普遍性，我們可以假定 $p \nmid a_k$. 若 $f(\lambda x + \mu) - f(\mu)$ 與 $f(x)$ 全同，mod p，則

$$a_k \lambda^k \equiv a_k, \qquad k a_k \lambda^{k-1} \mu + a_{k-1} \lambda^{k-1} \equiv a_{k-1} \pmod p.$$

由定理 2.9.1，$\lambda^k \equiv 1 \pmod p$ 之根數至多爲 k，對於固定之 λ，卽唯一的決定 μ. 故形如 $f(\lambda x + \mu) - f(\mu)$ 之多項式至多有 k 個與 $f(x)$ 全同，mod p. 也就是說，至少有 $p(p-1)/k$ 個互不相同的多項式 $f(\lambda x + \mu) - f(\mu)$. 故得

$$\frac{p(p-1)}{k} |S(p, f(x))|^{2k} \leqslant k!\, p^{2k},$$

卽

$$|S(p, f(x))| \leqslant \left(\frac{k \cdot k!}{p(p-1)}\right)^{\frac{1}{2k}} p \leqslant (2k \cdot k!)^{\frac{1}{2k}} p^{1-\frac{1}{k}}.$$

設 $l > 1$, $p^l \| (k a_k, \cdots, 2a_2, a_1)$. 又設 $\mu_1, \cdots, \mu_r$ 爲

$$f'(x) \equiv 0 \pmod{p^{l+1}}, \qquad 0 \leqslant x < p$$

之相異的根，其重數分別爲 $m_1, \cdots, m_r$. 命 $m_1 + \cdots + m_r = m$，易見 $m \leqslant k-1$. 今證明

$$|S(p^l, f(x))| \leqslant k^2 \max(1, m)\, p^{\left(1-\frac{1}{k}\right)l}.$$

由假定 $p \nmid (a_k, \cdots, a_1)$，$p^t | (ka_k, \cdots, 2a_2, a_1)$，故必 $p^t \leqslant k$.

1) $l < 2(t+1)$. 因 $l > 1$, 故 $t \geqslant 1$. 卽得

$$|S(p^l, f(x))| \leqslant p^l \leqslant p^{l\left(1-\frac{1}{k}\right)} \cdot p^{(2t+1)\frac{1}{k}} \leqslant p^{l\left(1-\frac{1}{k}\right)} k^{\left(2+\frac{1}{t}\right)\frac{1}{k}} \leqslant k^2 p^{l\left(1-\frac{1}{k}\right)},$$

故此時定理成立.

2) $l \geqslant 2(t+1)$. 寫

$$S(p^l, f(x)) = \sum_{\nu=1}^{p} \sum_{\substack{0 \leqslant x \leqslant p^l-1 \\ x \equiv \nu \pmod p}} e_{p^l}(f(x)) = \sum_{\nu=1}^{p} S_\nu.$$

若 ν 非 μ_i 之一，則命

$$x = y + p^{l-t-1} z, \qquad 0 \leqslant y < p^{l-t-1}, \qquad 0 \leqslant z < p^{t+1}.$$

由 $f'(y) \not\equiv 0 \pmod{p^{t+1}}$ 及定理 1.1, 卽得

$$S_\nu = \sum_{\substack{0 \leqslant x < p^l \\ x \equiv \nu \pmod p}} e_{p^l}(f(x)) = \sum_{\substack{0 \leqslant y < p^{l-t-1} \\ y \equiv \nu \pmod p}} \sum_{0 \leqslant z < p^{t+1}} e_{p^l}(f(y) - p^{l-t-1} f'(y)\, z) =$$

$$= \sum_{\substack{0 \leqslant y < p^{l-t-1} \\ y \equiv \nu \pmod p}} e_{p^l}(f(y)) \sum_{0 \leqslant z < p^{t+1}} e_{p^{t+1}}(z f'(y)) = 0. \tag{3}$$

若 $\nu = \mu_i$, 則依引 2 定義 σ_i, 卽得

$$S_{\mu_i} = \sum_{\substack{x=1 \\ x \equiv \mu_i \pmod p}}^{p^l} e_{p^l}(f(x)) = \sum_{y=1}^{p^{l-1}} e_{p^l}(f(\mu_i + py)) =$$

$$= e_{p^l}(f(\mu_i)) \sum_{y=1}^{p^{l-1}} e_{p^{l-\sigma_i}}(p^{-\sigma_i}(f(\mu_i + py) - f(\mu_i))).$$

命 $g_i = p^{-\sigma_i}(f(\mu_i + py) - f(\mu_i))$. 由引 2,

$$|S_{\mu_i}| = p^{\sigma_i - 1} |S(p^{l-\sigma_i}, g_i(x))| \leqslant p^{\sigma_i\left(1-\frac{1}{k}\right)} |S(p^{l-\sigma_i}, g_i(x))|. \tag{4}$$

由 (3) 及 (4) 得

$$|S(p^l, f(x))| \leqslant \sum_{i=1}^{r} p^{\sigma_i\left(1-\frac{1}{k}\right)} |S(p^{l-\sigma_i}, g_i(x))|.$$

若 $l \geqslant \max(\sigma_1, \cdots, \sigma_r)$. 則由歸納法之假定及引 1，由上式卽得

$$|S(p^l, f(x))| \leqslant \sum_{i=1}^{r} m_i p^{\sigma_i\left(1-\frac{1}{k}\right)} k^2 p^{(l-\sigma_i)\left(1-\frac{1}{k}\right)} < mk^2 p^{l\left(1-\frac{1}{k}\right)}.$$

若 $l < \max(\sigma_1, \cdots, \sigma_r)$，則 $l < k$,

$$|S(p^l, f(x))| \leqslant \sum_{i=1}^{r} p^{\sigma_i-1} p^{l-\sigma_i} \leqslant k p^{l\left(1-\frac{1}{k}\right)}.$$

基本定理證畢.

定理 1 之證明: 設 $q = p_1^{l_1} \cdots p_s^{l_s}$, $p_1, \cdots, p_s$ 是相異的素數. 由定理 2,

$$S(q, f(x)) = \prod_{p \mid q} S\left(p^l, \frac{f(qx/p^l)}{q/p^l}\right),$$

由基本引理,

$$|S(q, f(x))| \leqslant C_1^s q^{1-\frac{1}{k}}$$

由定理 6.6.2 (我們可設 $C_1 > 1$)

$$C_1^s = (2^s)^{\log C_1/\log 2} \leqslant C_2(k, \varepsilon) q^{\varepsilon}.$$

定理得證.

第　八　章

與橢圓模函數有關的幾個數論問題

§1. 引言. 在橢圓模函數論中常論及以下的四個重要函數:

$$q_0 = \prod_{n=1}^{\infty} (1 - q^{2n}),$$

$$q_1 = \prod_{n=1}^{\infty} (1 + q^{2n}),$$

$$q_2 = \prod_{n=1}^{\infty} (1 + q^{2n-1}),$$

$$q_3 = \prod_{n=1}^{\infty} (1 - q^{2n-1}).$$

此處爲尊重橢圓模函數論中之習慣, 以 q 表變數, 可能是實數也可能是複數, $|q| < 1$. 此時這四個無窮乘積顯然收斂.

本章之目的並不深入討論橢圓模函數之性質, 甚且並無橢圓模函數之定義, 而僅圍繞數論上之具體問題: 整數之分拆問題, 四平方和問題, 而討論與 q_0, q_1, q_2, q_3 有關之冪級數變化. 又本章中所涉及之收斂問題, 皆極淺顯, 凡熟悉高等微積分之讀者都能易於補足*), 因此, 在本節中略去所有關於收斂性之討論.

q_1, q_2, q_3 之間有次之簡單關係.

定理 1. 若 $|q| < 1$, 則

$$q_1 q_2 q_3 = 1.$$

證: 已知

$$q_2 q_3 = \prod_{n=1}^{\infty} (1 - q^{2(2n-1)}).$$

在 q_1 中依 $2n$ 中所包有 2 之乘方之次數重新排列, 得

*) 在 §8 中還用到了高等微積分中關於 n 重積分的計算.

$$q_1=\prod_{n=1}^{\infty}(1+q^{2(2n-1)})\prod_{n=1}^{\infty}(1+q^{4(2n-1)})\prod_{n=1}^{\infty}(1+q^{8(2n-1)})\cdots.$$

由此可見

$$q_1q_2q_3=\prod_{n=1}^{\infty}(1-q^{2(2n-1)})\prod_{n=1}^{\infty}(1+q^{2(2n-1)})\prod_{n=1}^{\infty}(1+q^{4(2n-1)})\prod_{n=1}^{\infty}(1+q^{8(2n-1)})\cdots=$$

$$=\prod_{n=1}^{\infty}(1-q^{4(2n-1)})\prod_{n=1}^{\infty}(1+q^{4(2n-1)})\prod_{n=1}^{\infty}(1+q^{8(2n-1)})\cdots=$$

$$=\prod_{n=1}^{\infty}(1-q^{8(2n-1)})\prod_{n=1}^{\infty}(1+q^{8(2n-1)})\cdots=\cdots=1$$

定理還可由下面的等式得出:

$$q_0q_1q_2q_3=\prod_{n=1}^{\infty}(1-q^n)\prod_{n=1}^{\infty}(1+q^n)=\prod_{n=1}^{\infty}(1-q^{2n})=q_0.$$

§2. 整數分拆. 命 n 是一正整數. 把 n 分成若干個正整數之和之一法名爲 n 之一種分拆. 例如:

$$5=4+1=3+2=3+1+1=2+2+1=$$
$$=2+1+1+1=1+1+1+1+1,$$

故 5 之分拆有 7.

以 $p(n)$ 表 n 之分拆之種數, 則上例說明 $p(5)=7$.

若限定分拆中每一部分不超過 r, 則此類之分拆數以 $p_r(n)$ 表之. 例如 $p_3(5)=5$.

定理 1. 若 $|q|<1$, 則

$$1+\sum_{n=1}^{\infty}p_r(n)\,q^n=\frac{1}{(1-q)(1-q^2)\cdots(1-q^r)}.$$

證: 上式之右邊等於

$$(1+q+q^2+q^3+\cdots+q^{x_1}+\cdots)\times$$
$$\times(1+q^2+(q^2)^2+(q^2)^3+\cdots+(q^2)^{x_2}+\cdots)\times$$
$$\times(1+q^3+(q^3)^2+(q^3)^3+\cdots+(q^3)^{x_3}+\cdots)\times$$
$$\times\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\times$$
$$\times(1+q^r+(q^r)^2+(q^r)^3+\cdots+(q^r)^{x_r}+\cdots),$$

其中 q^n 之係數乃

$$x_1+2x_2+3x_3+\cdots+rx_r=n$$

之非負整數解答數,也就是 $p_r(n)$.

用與此相同之原則,吾人可證:

定理 2. 若 $|q|<1$, 則

$$\frac{1}{q_0q_3}=\frac{1}{(1-q)(1-q^2)(1-q^3)\cdots}=$$

$$=1+\sum_{n=1}^{\infty}p(n)q^n.$$

定理 3. 命 $q(n)$ 表示把 n 分爲若干個奇數之和之分拆之種數,則

$$\frac{1}{q_3}=\frac{1}{(1-q)(1-q^3)(1-q^5)\cdots}=1+\sum_{n=1}^{\infty}q(n)q^n.$$

定理 4. $q_1\,q_2$ 展開式中 q^n 之係數等於把 n 分爲不相等部分之分拆之種數.

此三定理之證明讀者不難補出. 由定理 1.1 並結合定理 3,4 之結果, 可得

定理 5. 把 n 分爲不等數之和之分拆數等於把 n 分爲奇數之和之分拆數.

§ 3. Jacobi 等式.

定理 1. 若 $|q|<1$, $z\neq 0$, 則有

$$\prod_{n=1}^{\infty}((1-q^{2n})(1+q^{2n-1}z)(1+q^{2n-1}z^{-1}))=1+\sum_{n=1}^{\infty}q^{n^2}(z^n+z^{-n})=$$

$$=\sum_{n=-\infty}^{\infty}q^{n^2}z^n. \qquad (1)$$

證: 此二級數顯然相等.

命

$$\varphi_m(z)=\prod_{n=1}^{m}\{(1+q^{2n-1}z)(1+q^{2n-1}z^{-1})\}=$$

$$=X_0+X_1(z+z^{-1})+X_2(z^2+z^{-2})+\cdots+X_m(z^m+z^{-m}), \qquad (2)$$

此處 $X_0, X_1, \cdots, X_m$ 與 z 無關.

Z^m 之係數顯然等於

$$X_m = q^{1+3+\cdots+(2m-1)} = q^{m^2}. \tag{3}$$

又

$$\varphi_m(q^2 z) = \prod_{n=1}^{m} \{(1+q^{2n+1}z)(1+q^{2n-3}z^{-1})\} =$$
$$= \frac{1+q^{-1}z^{-1}}{1+qz} \cdot \frac{1+q^{2m+1}z}{1+q^{2m-1}z^{-1}} \varphi_m(z) =$$
$$= \frac{1+q^{2m+1}z}{qz+q^{2m}} \varphi_m(z),$$

即

$$(qz + q^{2m})\varphi_m(q^2 z) = (1+q^{2m+1}z)\varphi_m(z).$$

將 (2) 式代入,而比較 z^{1-n} 之係數可知

$$X_n = \frac{q^{2n-1}(1-q^{2m-2n+2})}{1-q^{2m+2n}} X_{n-1},$$

亦即

$$X_n = q^{n^2} \frac{(1-q^{2m-2n+2})(1-q^{2m-2n+4})\cdots(1-q^{2m})}{(1-q^{2m+2n})(1-q^{2m+2n-2})\cdots(1-q^{2m+2})} X_0.$$

由 (3) 可知

$$X_0 = \frac{(1-q^{4m})(1-q^{4m-2})\cdots(1-q^{2m+2})}{(1-q^2)(1-q^4)\cdots(1-q^{2m})},$$

故當 $0 \leqslant n \leqslant m-1$ 時,

$$X_n = \frac{q^{n^2}}{(1-q^2)(1-q^4)\cdots(1-q^{2m})} X_n',$$

此處

$$X_n' = \frac{(1-q^{2m-2n+2})(1-q^{2m-2n+4})\cdots(1-q^{2m})}{(1-q^{2m+2n})(1-q^{2m+2n-2})\cdots(1-q^{2m+2})}(1-q^{2m+2})\cdots(1-q^{4m}) =$$
$$= (1-q^{2m-2n+2})\cdots(1-q^{2m})(1-q^{2m+2n+2})\cdots(1-q^{4m}). \tag{4}$$

因此 (2) 式可以寫成

$$(1-q^2)(1-q^4)\cdots(1-q^{2m})\varphi_m(z) = X_0' + \sum_{n=1}^{m} q^{n^2}(z^n+z^{-n})X_n'. \tag{5}$$

當 $m\to\infty$, 則 $X_n'\to 1$, 故形式上已得出定理中之等式,但對於逐項取限之可能性還須加以證明.

命

$$u_{0,m} = X_0,$$

$$u_{n,m}\begin{cases}=\dfrac{q^{n^2}}{(1-q^2)(1-q^4)\cdots(1-q^{2m})}X_n'(z^n+z^{-n}), & 若\quad 1\leqslant n\leqslant m,\\ =0, & 若\quad n>m,\end{cases}$$

則

$$\varphi_m(z)=\sum_{n=0}^{\infty}u_{n,m}. \tag{6}$$

當 $m\to\infty$ 時，其公項

$$u_{n,m}\to u_n,$$

此處

$$u_0=\frac{1}{(1-q^2)(1-q^4)\cdots},\qquad u_n=\frac{q^{n^2}(z^n+z^{-n})}{(1-q^2)(1-q^4)\cdots}\quad (n>0).$$

今有

$$|X_n'|<\prod_{k=1}^{\infty}(1+|q|^{2k})=K_1\quad (定義)$$

及

$$\left|\frac{1}{(1-q^2)(1-q^4)\cdots(1-q^{2m})}\right|<\prod_{k=1}^{\infty}\frac{1}{1-|q|^{2k}}=K_2\ (定義),$$

故

$$|u_{n,m}|\leqslant K_1K_2|q|^{n^2}(|z|^n+|z|^{-n})=v_n.$$

v_n 與 m 無關，且由於當 $n\to\infty$ 時，

$$\frac{v_{n+1}}{v_n}=|q|^{2n+1}\left(\frac{|z|^{n+1}+|z|^{-(n+1)}}{|z|^n+|z|^{-n}}\right)<$$
$$<|q|^{2n+1}(|z|+|z|^{-1})\to 0,$$

故 $\Sigma\, v_n$ 是收斂的. 卽級數 (6) 對 m 是一致收斂的. 因此

$$\varphi_m(z)\to\sum_{0}^{\infty}u_n.$$

此補足了可能逐項求限的證明.

定理 1 包有不少有趣的特例:

分別取 $z=\pm 1$ 及 $z=q$, 則得:

定理 2. 當 $|q|<1$, 時

$$q_0\,q_2^2=\sum_{n=-\infty}^{\infty}q^{n^2}$$

及

$$q_0 q_3^2 = \sum_{n=-\infty}^{\infty} (-1)^n q^{n^2},$$

$$q_0 q_1^2 = \sum_{n=0}^{\infty} q^{n^2+n}.$$

以 $-q^{3/2}$ 代 q 及取 $z = q^{\frac{1}{2}}$, 則得

$$\prod_{n=1}^{\infty} ((1-q^{3n})(1-q^{3n-1})(1-q^{3n-2}))=$$

$$= \sum_{n=-\infty}^{\infty} (-q^{\frac{3}{2}})^{n^2} (q^{\frac{n}{2}})=$$

$$= \sum_{n=-\infty}^{\infty} (-1)^n q^{\frac{1}{2}(3n^2+n)},$$

卽得 Euler 公式:

定 理 3. 若 $|q| < 1$, 則

$$q_0 q_3 = (1-q)(1-q^2)(1-q^3)\cdots =$$

$$= \sum_{n=-\infty}^{\infty} (-1)^n q^{\frac{1}{2}n(3n+1)} = 1 + \sum_{n=1}^{\infty} (-1)^n (q^{\frac{1}{2}n(3n-1)} + q^{\frac{1}{2}n(3n+1)})=$$

$$= 1 - q - q^2 + q^5 + q^7 - q^{12} - q^{15} + \cdots.$$

再取 $q^{\frac{1}{2}}$ 代 q, $q^{\frac{1}{2}}$ 代 z, 則得

$$\prod_{n=1}^{\infty} (1-q^n)(1+q^n)(1+q^{n-1}) = \sum_{n=-\infty}^{\infty} q^{\frac{1}{2}(n^2+n)},$$

卽得:

定 理 4. 若 $|q| < 1$, 則

$$q_0 q_1 q_2 = \sum_{n=0}^{\infty} q^{\frac{1}{2}n(n+1)}.$$

注意:指數 $\frac{1}{2}n(n+1)$ 乃普通所謂之三角數. 由定理 1.1, 定理 4 也可重述爲:

定 理 5. 若 $|q| < 1$, 則

$$\frac{q_0}{q_3} = \frac{(1-q^2)(1-q^4)\cdots}{(1-q)(1-q^3)\cdots} = \sum_{n=0}^{\infty} q^{\frac{1}{2}n(n+1)}.$$

今往證明：

定理 6. 若 $|q|<1$，則

$$(q_0\,q_3)^3=((1-q)(1-q^2)(1-q^3)\cdots)^3=$$

$$=\sum_{n=-\infty}^{\infty}(-1)^n\,n\,q^{\frac{1}{2}n(n+1)}=$$

$$=1-3q+5q^3-7q^6+\cdots.$$

證： 在定理 1 中以 $q^{\frac{1}{2}}$ 代 q，以 $q^{\frac{1}{2}}\zeta$ 代 z，則得

$$\prod_{n=1}^{\infty}((1-q^n)(1+q^n\zeta)(1+q^{n-1}\zeta^{-1}))=\sum_{n=-\infty}^{\infty}q^{\frac{1}{2}n(n+1)}\zeta^n,$$

即

$$\frac{\zeta+1}{\zeta}\prod_{n=1}^{\infty}((1-q^n)(1+q^n\zeta)(1+q^n\zeta^{-1}))=\sum_{n=-\infty}^{\infty}q^{\frac{1}{2}n(n+1)}\zeta^n.$$

今往討論 $\zeta\to-1$ 時之情況．顯然有

$$\lim_{\zeta\to-1}\prod_{n=1}^{\infty}((1-q^n)(1+q^n\zeta)(1+q^n\zeta^{-1}))=\left(\prod_{n=1}^{\infty}(1-q^n)\right)^3.$$

由於

$$\sum_{n=-\infty}^{\infty}(-1)^n q^{\frac{1}{2}n(n+1)}=\sum_{n=0}^{\infty}(-1)^n q^{\frac{1}{2}n(n+1)}+\sum_{n=-\infty}^{-1}(-1)^n q^{\frac{1}{2}n(n+1)}=$$

$$=\sum_{n=0}^{\infty}(-1)^n q^{\frac{1}{2}n(n+1)}+\sum_{m=0}^{\infty}(-1)^{m+1}q^{\frac{1}{2}m(m+1)}=0.$$

可知

$$\frac{\zeta}{\zeta+1}\sum_{n=-\infty}^{\infty}q^{\frac{1}{2}n(n+1)}\zeta^n=$$

$$=\frac{\zeta}{\zeta+1}\sum_{n=-\infty}^{\infty}q^{\frac{1}{2}n(n+1)}(\zeta^n-(-1)^n)=$$

$$=\sum_{n=-\infty}^{\infty}q^{\frac{1}{2}n(n+1)}\frac{\zeta(\zeta^n-(-1)^n)}{\zeta+1}.$$

因爲

$$\lim_{\zeta\to-1}\frac{(\zeta^n-(-1)^n)}{\zeta+1}=n(-1)^{n-1},$$

可知

$$\lim_{\zeta\to -1}\frac{\zeta}{\zeta+1}\sum_{n=-\infty}^{\infty} q^{\frac{1}{2}n(n+1)}\zeta^n=\sum_{n=-\infty}^{\infty}(-1)^n n\, q^{\frac{1}{2}n(n+1)}.$$

故得定理. (其中用及兩次逐項求限法,皆可用一致收斂性證實之.)

習題 1. 求證當 $|q|<1$ 時,

$$\prod_{n=0}^{\infty}((1-q^{5n+1})(1-q^{5n+4})(1-q^{5n+5}))=\sum_{n=-\infty}^{\infty}(-1)^n q^{\frac{1}{2}n(5n+3)},$$

$$\prod_{n=0}^{\infty}((1-q^{5n+2})(1-q^{5n+3})(1-q^{5n+5}))=\sum_{n=-\infty}^{\infty}(-1)^n q^{\frac{1}{2}n(5n+1)}.$$

習題 2. 證明

$$q(1-q^{24})(1-q^{2\cdot 24})(1-q^{3\cdot 24})\cdots=q^{1^2}-q^{5^2}-q^{7^2}+q^{11^2}+q^{13^2}-q^{17^2}-\cdots,$$
$$q((1-q^8)(1-q^{2\cdot 8})(1-q^{3\cdot 8})\cdots\cdots)^3=q^{1^2}-3q^{3^2}+5q^{5^2}-7q^{7^2}+\cdots.$$

§4. 分式表示法.

定理 1. 若 $|q|<1$, 則

$$(1+aq)(1+aq^3)(1+aq^5)\cdots=1+\frac{aq}{1-q^2}+\frac{a^2q^4}{(1-q^2)(1-q^4)}+\cdots+$$
$$+\frac{a^m q^{m^2}}{(1-q^2)\cdots(1-q^{2m})}+\cdots.$$

證: 命 $F(a)$ 代表上式之左端,且命

$$F(a)=1+c_1a+c_2a^2+\cdots.$$

由於

$$(1+aq)F(aq^2)=(1+aq)(1+aq^3)(1+aq^5)\cdots=$$
$$=F(a),$$

比較此式中 a^n 之係數可知

$$c_1=q+c_1q^2,\qquad c_2=c_1q^3+c_2q^4,\cdots$$
$$c_m=c_{m-1}q^{2m-1}+c_mq^{2m},\cdots$$

故

$$c_m=\frac{q^{2m-1}}{1-q^{2m}}c_{m-1}=\frac{q^{1+3+\cdots+(2m-1)}}{(1-q^2)(1-q^4)\cdots(1-q^{2m})}=$$
$$=\frac{q^{m^2}}{(1-q^2)(1-q^4)\cdots(1-q^{2m})}.$$

此即定理.

在定理中各取 $a=1$ 及 $a=q$，可得以下之二定理:

定理 2. 當 $|q|<1$，則

$$q_2=(1+q)(1+q^3)(1+q^5)\cdots=$$

$$=1+\frac{q}{1-q^2}+\frac{q^4}{(1-q^2)(1-q^4)}+\cdots+\frac{q^{m^2}}{(1-q^2)(1-q^4)\cdots(1-q^{2m})}+\cdots.$$

定理 3. 當 $|q|<1$，則

$$q_1=(1+q^2)(1+q^4)(1+q^6)\cdots=$$

$$=1+\frac{q^2}{1-q^2}+\frac{q^6}{(1-q^2)(1-q^4)}+\cdots+\frac{q^{m^2+m}}{(1-q^2)(1-q^4)\cdots(1-q^{2m})}+\cdots.$$

或以 $q^{\frac{1}{2}}$ 代 q，以 $q^{\frac{1}{2}}$ 代 a，卽得:

定理 4. 當 $|q|<1$，則

$$(1+q)(1+q^2)(1+q^3)\cdots=$$

$$=1+\frac{q}{1-q}+\frac{q^3}{(1-q)(1-q^2)}+\cdots+\frac{q^{\frac{1}{2}m(m+1)}}{(1-q)(1-q^2)\cdots(1-q^m)}+\cdots.$$

定理 5. 當 $|q|<1$ 時,

$$\frac{1}{(1-aq)(1-aq^2)(1-aq^3)\cdots}=$$

$$=1+\frac{aq}{1-q}+\frac{a^2q^2}{(1-q)(1-q^2)}+\frac{a^3q^3}{(1-q)(1-q^2)(1-q^3)}+\cdots.$$

證: 命上式之左端爲 $F(a)$，則

$$F(aq)=\frac{1}{(1-aq^2)(1-aq^3)\cdots}=$$

$$=(1-aq)F(a).$$

以展開式

$$F(a)=1+\sum_{m=1}^{\infty}c_m a^m$$

代入上式，則得

$$c_m q^m=c_m-c_{m-1}q,$$

卽

$$c_m=\frac{q}{1-q^m}c_{m-1}.$$

故得

$$c_m=\frac{q^m}{(1-q)(1-q^2)\cdots(1-q^m)}.$$

此定理之特例爲:

定理 6. 當 $|q|<1$, 則

$$\frac{1}{q_0q_3}=1+\frac{q}{1-q}+\frac{q^2}{(1-q)(1-q^2)}+\frac{q^3}{(1-q)(1-q^2)(1-q^3)}+\cdots.$$

在定理 5 中以 q^2 代 q, 以 q^{-1} 代 a, 則得

定理 7. 當 $|q|<1$ 時,

$$\frac{1}{q_3}=1+\frac{q}{1-q^2}+\frac{q^2}{(1-q^2)(1-q^4)}+\frac{q^3}{(1-q^2)(1-q^4)(1-q^6)}+\cdots.$$

§5. 分拆之圖解法.

設有一 n 分拆

$$n=a_1+a_2+a_3+\cdots+a_s,$$

其中之 a_i 按由大而小之次序排列,卽

$$a_1\geqslant a_2\geqslant a_3\geqslant\cdots\geqslant a_s.$$

我們作一圖形,其第一行有 a_1 個點,第二行有 a_2 個點, …, 每行之排頭看齊,以後等距,如此之點圖稱爲此分拆之圖解. 例如:

```
• • • • • • •
• • • •
• • •
• • •
•
```

就是分拆

$$18=7+4+3+3+1$$

之圖解. 以上之圖解固然可以逐行讀出, 但也可以逐列讀出. 如此得另一分拆. 此分拆謂之原分拆之共軛分拆. 上圖之共軛分拆爲

$$18=5+4+4+2+1+1+1.$$

橫看豎看,可有次之定理:

定理 1. 把 n 分爲每份不超過 m 之分拆數等於把 n 分爲不超過 m 份之分拆數.

分拆圖表法還能證明更複雜之定理. 例如:

定理 4.2 之另證:

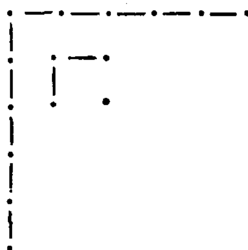
顯然

$$(1+q)(1+q^3)(1+q^5)\cdots$$

之展開式中 q^n 之係數等於把 n 分爲不等的奇數之和之分拆數 $r(n)$. 例如

$$15=11+3+1=9+5+1=7+5+3.$$

今將 $15=11+3+1$ 之圖表重新排列如下圖:



由於每份是奇數且各不相等,故列出之後該圖仍爲一分拆圖. 但此圖有一特別性質,橫看縱看都是一樣. 此種圖形謂之自共軛圖形,所對應之分拆謂之自共軛分拆. 故有一不等的奇數之和的分拆一定有一自共軛分拆,且反之亦眞.

故 $r(n)$ 乃 n 之自共軛分拆數. 任一自共軛圖形所包有之極大的正方塊其邊長設爲 t (上圖中 $t=3$). 則對一固定 t 之自共軛分拆之種數等於

$$\frac{n-t^2}{2}$$

之不超過 t 份之分拆數. 這就是

$$\frac{q^{t^2}}{(1-q^2)(1-q^4)\cdots(1-q^{2t})}$$

之展開式中 q^n 之係數. 因此得

$$(1+q)(1+q^3)(1+q^5)\cdots=$$

$$=\sum_{t=0}^{\infty}\frac{q^{t^2}}{(1-q^2)(1-q^4)\cdots(1-q^{2t})},$$

式中對應於 $t=0$ 之項爲 1. 此卽定理 4.2.

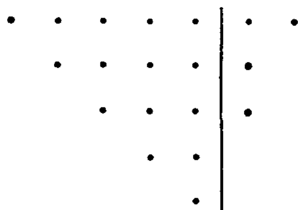
習題 1. 證明

$$\frac{1}{(1-q)(1-q^2)(1-q^3)\cdots}=1+\frac{q}{(1-q)^2}+\frac{q^4}{(1-q)^2(1-q^2)^2}+$$
$$+\frac{q^9}{(1-q)^2(1-q^2)^2(1-q^3)^2}+\cdots.$$

習題 2. 用圖表法證明定理 4.4.

提示：把一分成不等部分之分拆每行縮一格排列，例如

$$19=7+5+4+2+1$$



再看直線右邊之分拆.

分拆圖表法之另一應用在證明定理 3.3. 此定理顯然可以改述爲：

定理 2. 命 $E(n)$ 代表把 n 分爲偶數個不等數之和(偶分拆) 之分拆數，$U(n)$ 代表把 n 分爲奇數個不等數之和 (奇分拆) 之分拆數，則

$$E(n)-U(n)=\begin{cases}0, & 若\quad n\neq\frac{1}{2}k(3k\pm 1),\\(-1)^k, & 若\quad n=\frac{1}{2}k(3k\pm 1).\end{cases}$$

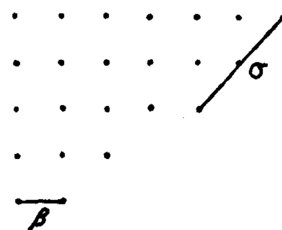


圖 1

證 (Franklin)： 我們在 n 之一分拆之圖解中，於其右上角之終點向左下角引一 45° 之斜線，此線之終點爲其與圖形相遇之終點，此線以 σ 記之. 我們又用線連接圖形之最下一行，此線以 β 記之.

我們可以將 β 移於圖形之右上角，置於 σ 之右面而與 σ 平行 (這種手續以 O 記之)，也可以將 σ 移置於 β 之下而與 β 平行 (這種手續以 Ω 記之). 對於一移動 O 或 Ω，我們可以得一分拆，但也可能得到一個圖形，它不能表示一分拆 (這裏用來表示分拆的圖形皆是由大至小排列). 如上圖 1，經 O 我們得圖 2，經 Ω 我們得圖 3，在我們的規定下，圖 2 是一分拆的圖解，而圖 3 則否.

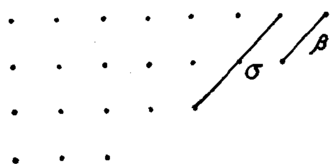


圖 2

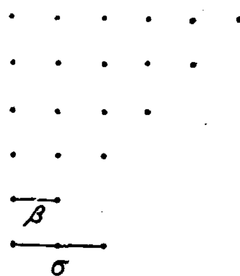


圖 3

現分三種情形論之:

1) $\beta<\sigma$. 由圖 1 可以看出 O 常爲可能,而 Ω 則不可能.

2) $\beta>\sigma$. 此時 O 常爲不可能. 又除 β 與 σ 相遇且 $\beta=\sigma+1$ 之情形外 (圖 4), Ω 常爲可能. 對除外之情形,所得者有二部分相同,非我們所需.

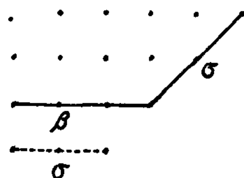


圖 4

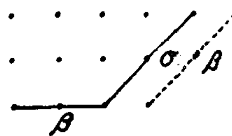


圖 5

3) $\beta=\sigma$. 此時除 β 與 σ 相遇之情形 (圖 5) 外, O 常爲可能. 對除外之情形, O 顯然不可能. Ω 則常不可能.

由是可以看出,若對於一種分拆, O 與 Ω 有一可能,有一不可能,則我們卽能由一偶 (或奇) 分拆得到一奇 (或偶) 分拆,卽在此種情形,偶分拆與奇分拆之間卽建立 (1,1) 對應,但對於圖 4 與圖 5 之情形,此種對應卽不可能. 對於前一種情形, n 必爲

$$n=(k+1)+(k+2)+\cdots+2k=\frac{1}{2}(3k^2+k),$$

對於後一種情形,

$$n=k+(k+1)+\cdots+(2k-1)=\frac{1}{2}(3k^2-k),$$

無論是前一種情形或後一種情形,皆顯然有 $E(n)-U(n)=(-1)^k$.

§6. $p(n)$ 之估値.

在本節中將先用最簡單之代數方法以得出 $p(n)$ 最粗略之估值, 再用略精

深之方法以得出 $\log p(n)$ 之無窮大之階，但再深入用所謂 Tauber 型方法以得出 $p(n)$ 無窮大之階，以及更深入用模函數論之結果及解析數論之方法以求出 $p(n)$ 之展開式則不在本書範圍之內．在這逐步求精之方法中極易體會出各種方法之深入度．

定理 1. 當 $n>1$ 時，

$$2^{[\sqrt{n}]}<p(n)<n^{3[\sqrt{n}]}.$$

證：1）先證左式．在

$$1,2,\cdots,[\sqrt{n}]$$

中任取 r 個 $a_1,\cdots,a_r$，而作一分拆

$$n=a_1+\cdots+a_r+(n-a_1-\cdots-a_r). \tag{1}$$

由於

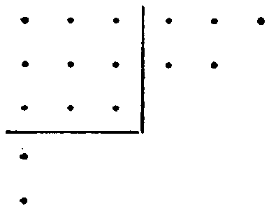
$$a_1+\cdots+a_r\leqslant 1+2+\cdots+[\sqrt{n}]\leqslant$$
$$\leqslant[\sqrt{n}]^2\leqslant n,$$

故 (1) 式是一分拆．總共有

$$1+\binom{[\sqrt{n}]}{1}+\binom{[\sqrt{n}]}{2}+\cdots+\binom{[\sqrt{n}]}{r}+\cdots=(1+1)^{[\sqrt{n}]}=2^{[\sqrt{n}]}$$

種取法，故得定理中之左式．

2）後證右式．今討論 n 之分拆圖解



圖中左上角最大正方形之邊長爲 r．圖中右上角之 r 列對應於一個不大於 $n-r^2$ 之整數之分拆，左下角亦然．故如 r 固定，右上角之可能性 $\leqslant n^r$，左下角亦然．故得（顯然 $r\leqslant[\sqrt{n}]$）

$$p(n)\leqslant\sum_{r=1}^{[\sqrt{n}]}n^{2r}<\sqrt{n}\,n^{2[\sqrt{n}]}<n^{3[\sqrt{n}]}.$$

定理 2.

$$\lim_{n\to\infty}\frac{\log p(n)}{n^{1/2}}=\pi\sqrt{\frac{2}{3}}.$$

證此定理需要以下諸預備定理.

定理 3.

$$np(n)=\sum_{lk\leqslant n} lp(n-lk).$$

證: 設 $|q|<1$, 命

$$f(q)=\frac{1}{(1-q)(1-q^2)(1-q^3)\cdots}=$$

$$=1+\sum_{l=1}^{\infty}p(l)\,q^l.$$

用乘積式求 $f(q)$ 之對數之導數,則得

$$\frac{f'(q)}{f(q)}=\sum_{l=1}^{\infty}\frac{lq^{l-1}}{1-q^l}=$$

$$=\frac{1}{q}\sum_{l=1}^{\infty}l(q^l+q^{2l}+q^{3l}+\cdots)=$$

$$=\frac{1}{q}\sum_{l=1}^{\infty}\sum_{k=1}^{\infty}lq^{lk}.$$

又用 $f(q)$ 之冪級數展開式求微分可知

$$\sum_{n=1}^{\infty}np(n)q^n=qf'(q)=f(q)\sum_{l=1}^{\infty}\sum_{k=1}^{\infty}lq^{lk}=$$

$$=\left(1+\sum_{v=1}^{\infty}p(v)\,q^v\right)\sum_{l=1}^{\infty}\sum_{k=1}^{\infty}lq^{lk}.$$

比較係數,即得定理.

定理 4. 若 $n>v>0$, 則

$$\frac{1}{2}\frac{v}{\sqrt{n}}<n^{\frac{1}{2}}-(n-v)^{\frac{1}{2}}<\frac{1}{2}\frac{v}{\sqrt{n}}+\frac{v^2}{2n^{3/2}}.$$

證: 此可由下列不等式

$$1-\frac{x}{2}-\frac{x^2}{2}<(1-x)^{\frac{1}{2}}<1-\frac{x}{2},\qquad 0<x<1$$

得之. 而此不等式可由平方上式各項以證之. $\left(但須注意\ 1-\frac{x}{2}-\frac{x^2}{2}>0.\right)$

定 理 5. 若 $0<x<1$, 則

$$\frac{1}{x^2}-c_1<\frac{e^{-x}}{(1-e^{-x})^2}<\frac{1}{x^2},$$

此處 c_1 (及今後 $c_2, c_3, \cdots$) 皆表正常數.

證: 由

$$e^{\frac{1}{2}x}-e^{-\frac{1}{2}x}=x+\frac{2}{3!}\left(\frac{1}{2}x\right)^3+\frac{2}{5!}\left(\frac{1}{2}x\right)^5+\cdots>x$$

故得右邊之不等式. 因爲

$$\frac{1}{e^{\frac{1}{2}x}-e^{-\frac{1}{2}x}}=\frac{1}{x}(1+O(x^2)),$$

故得

$$\frac{1}{x^2}=\frac{e^{-x}}{(1-e^{-x})^2}+O(1).$$

此即定理中之左邊不等式.

定 理 6. 命 α 表一正數,則

$$\frac{\pi^2 n}{6\alpha^2}-c_2\sqrt{n}<\sum_{k=1}^{\infty}\sum_{l=1}^{\infty}l\,e^{-\alpha lkn^{-\frac{1}{2}}}<\frac{\pi^2 n}{6\alpha^2}.$$

正確地說,此 c_2 與 α 有關.

證: 由於 $\sum_{l=1}^{\infty}lx^l=\frac{x}{(1-x)^2}$, 故此重和等於

$$\sum_{k=1}^{\infty}\frac{e^{-\alpha kn^{-\frac{1}{2}}}}{(1-e^{-\alpha kn^{-\frac{1}{2}}})^2}. \tag{2}$$

由定理 5 之右邊不等式可知此和

$$<\sum_{k=1}^{\infty}\frac{1}{(\alpha k\,n^{-\frac{1}{2}})^2}=\frac{n}{\alpha^2}\sum_{k=1}^{\infty}\frac{1}{k^2}=\frac{\pi^2 n}{6\alpha^2}.$$

把 (2) 式分成二分和

$$\sum_{k=1}^{[\sqrt{n}]}+\sum_{k=[\sqrt{n}]+1}^{\infty}=\sum\nolimits_1+\sum\nolimits_2,$$

用定理 5 之左邊不等式,則得

$$\sum_1 > \sum_{k=1}^{[\sqrt{n}]} \frac{1}{(\alpha k n^{-\frac{1}{2}})^2} + O(\sqrt{n}) =$$

$$= \frac{n}{\alpha^2} \sum_{k=1}^{[\sqrt{n}]} \frac{1}{k^2} + O(\sqrt{n}) =$$

$$= \frac{\pi^2 n}{6\alpha^2} + O\left(n \sum_{k>\sqrt{n}} \frac{1}{k^2}\right) + O(\sqrt{n}) =$$

$$= \frac{\pi^2 n}{6\alpha^2} + O(\sqrt{n}).$$

用定理 5 之右邊不等式,則

$$\sum_2 = O\left(n \sum_{k>\sqrt{n}} \frac{1}{k^2}\right) = O(\sqrt{n}).$$

合之可得本定理.

定理 2 之證明: 命 $c = \pi\sqrt{\frac{2}{3}}$.

1) 先證

$$p(n) < e^{cn^{\frac{1}{2}}}. \tag{3}$$

當 $n = 1$ 時 (3) 式顯然成立. 今往用歸納法. 由定理 3 及歸納法之假定可知

$$n\, p(n) < \sum_{lk \leqslant n} l\, e^{c(n-lk)^{\frac{1}{2}}} <$$

$$< \sum_{lk \leqslant n} l\, e^{cn^{\frac{1}{2}} - \frac{c}{2} lkn^{-\frac{1}{2}}} < \qquad \text{(用定理 4)}$$

$$< e^{cn^{\frac{1}{2}}} \sum_{k=1}^{\infty} \sum_{l=1}^{\infty} l\, e^{-clk/(2n^{\frac{1}{2}})} <$$

$$< e^{cn^{\frac{1}{2}}} \frac{\pi^2 n}{6(c/2)^2} = n\, e^{cn^{\frac{1}{2}}}. \qquad \text{(用定理 6)}$$

卽得 (3) 式.

2) 再證: 任與一正數 ε, 必有一正數 A $(= A(\varepsilon))$ 存在使

$$p(n) > \frac{1}{A} e^{(c-\varepsilon)n^{\frac{1}{2}}}.$$

仍用歸納法,但 A 之選擇稍後自明. 由定理 3 與 4 及歸納法之假定,可知

$$n\, p(n) > \frac{1}{A} e^{(c-\varepsilon)n^{\frac{1}{2}}} \sum_{lk \leqslant n} l\, e^{-\frac{1}{2}(c-\varepsilon)(lkn^{-\frac{1}{2}} + l^2k^2 n^{-\frac{3}{2}})}. \tag{4}$$

因爲 $e^{-x} > 1 - x$, 所以此二重和

$$\geqslant \sum_{lk\leqslant n} l\, e^{-\frac{1}{2}(c-\varepsilon)lkn^{-\frac{1}{2}}}\left(1-\frac{1}{2}(c-\varepsilon)\frac{l^2k^2}{n^{3/2}}\right)=$$

$$=\sum_{lk\leqslant n} l\, e^{-\frac{1}{2}(c-\varepsilon)lkn^{-\frac{1}{2}}}-\frac{(c-\varepsilon)}{2n^{3/2}}\sum_{lk\leqslant n}k^2 l^3 e^{-\frac{1}{2}(c-\varepsilon)lkn^{-\frac{1}{2}}}=$$

$$=\sum\nolimits_1-\frac{c-\varepsilon}{2n^{3/2}}\sum\nolimits_2 \qquad (\text{定義}). \tag{5}$$

因爲對任一正數 t, 常有 $e^{-x}=O\left(\frac{1}{x^t}\right)$, 所以

$$\sum_{lk>n} l\, e^{-\frac{1}{2}(c-\varepsilon)lkn^{-\frac{1}{2}}}=O\left(n^{\frac{t}{2}}\sum_{lk>n} l^{1-\frac{t}{4}}k^{-\frac{1}{4}t}(lk)^{-\frac{3}{8}t}\right)=$$

$$=O\left(n^{-\frac{1}{8}t}\sum_{l=1}^{\infty}\sum_{k=1}^{\infty} l^{1-\frac{1}{8}t}k^{-\frac{1}{8}t}\right)=$$

$$=O\left(n^{-\frac{1}{8}t}\right), \qquad \text{若 } t>8. \tag{6}$$

由此式及定理 6 可知

$$\sum\nolimits_1 > \frac{2\pi^2 n}{3(c-\varepsilon)^2}-c_3\sqrt{n}=$$

$$=\frac{2\pi^2 n}{3c^2}+\frac{2\pi^2 n}{3}\left(\frac{1}{(c-\varepsilon)^2}-\frac{1}{c^2}\right)-c_3\sqrt{n}>$$

$$>(1+2\varepsilon c^{-1})\,n-c_3\sqrt{n}. \tag{7}$$

$\left(\text{此處用了 } \frac{1}{(c-\varepsilon)^2}-\frac{1}{c^2}=2\int_{c-\varepsilon}^{c}x^{-3}\,dx>2\varepsilon c^{-3}.\right)$

另一方面，由二項式定理及定理 5,

$$\sum\nolimits_2=\sum_{lk\leqslant n}k^2 l^3 e^{-\frac{1}{2}(c-\varepsilon)lkn^{-\frac{1}{2}}}\leqslant$$

$$\leqslant\sum_{k=1}^{n}k^2\sum_{l=1}^{\infty}l^3 e^{-\frac{1}{2}(c-\varepsilon)lkn^{-\frac{1}{2}}}\leqslant$$

$$\leqslant 12\sum_{k=1}^{n}k^2\frac{e^{-\frac{1}{2}(c-\varepsilon)kn^{-\frac{1}{2}}}}{\left(1-e^{-\frac{1}{2}(c-\varepsilon)kn^{-\frac{1}{2}}}\right)^4}=$$

$$=O\left(n\sum_{k=1}^{n}\frac{1}{\left(1-e^{-\frac{1}{2}(c-\varepsilon)kn^{-\frac{1}{2}}}\right)^2}\right). \tag{8}$$

分括弧中之和爲二部:

$$\sum_{k=1}^{n} = \sum_{k\leqslant\sqrt{n}} + \sum_{\sqrt{n}<k\leqslant n}.$$

在第一部分中, $\frac{1}{2}(c-\varepsilon)k\,n^{-\frac{1}{2}} < \frac{1}{2}c$, 又當 $x<\frac{1}{2}c$ 時,

$$1-e^{-x}=\int_0^x e^{-t}\,dt > e^{-\frac{1}{2}c}x,$$

卽得

$$\sum_{k\leqslant\sqrt{n}} \frac{1}{(1-e^{-\frac{1}{2}(c-\varepsilon)kn^{-\frac{1}{2}}})^2} = O\left(n\sum_{k\leqslant\sqrt{n}}\frac{1}{k^2}\right)=O(n).$$

在第二部分中, $\frac{1}{2}(c-\varepsilon)kn^{-\frac{1}{2}} \geqslant \frac{1}{2}(c-\varepsilon)$, 而

$$1-e^{-\frac{1}{2}(c-\varepsilon)kn^{-\frac{1}{2}}} > 1-e^{-\frac{1}{2}(c-\varepsilon)},$$

故得

$$\sum_{\sqrt{n}<k\leqslant n} \frac{1}{(1-e^{-\frac{1}{2}(c-\varepsilon)kn^{-\frac{1}{2}}})^2} = O\left(\sum_{k\leqslant n}1\right)=O(n).$$

由此及 (8) 可知

$$\sum\nolimits_2 = O(n^2). \tag{9}$$

總結 (4),(5),(7),(9),可得

$$n\,p(n) > \frac{1}{A}e^{(c-\varepsilon)n^{\frac{1}{2}}}\left((1+2\varepsilon c^{-1})n - c_4\sqrt{n}\right).$$

當

$$n > \left(\frac{c_4}{2\varepsilon c^{-1}}\right)^2$$

時,

$$p(n) > \frac{1}{A}e^{(c-\varepsilon)n^{\frac{1}{2}}}. \tag{10}$$

當 $n\leqslant c_4^2(2\varepsilon c^{-1})^{-2}$ 時,則取 A 相當大,使 (10) 式亦成立. 故得定理.

§ 7. 平方和問題.

命 $r_s(n)$ 代表

$$x_1^2+\cdots+x_s^2=n$$

之整數解答 $(x_1, \cdots, x_s)$ 之組數．由定理 6.7.5 已知

$$r_2(n) = 4\sum_{u|n}(-1)^{\frac{1}{2}(u-1)},$$

此處 u 過 n 之奇因子．此定理顯然與以下定理等價：

定理 1. 若 $|q|<1$，則

$$q_0^2 q_2^4 = \left(\sum_{n=-\infty}^{\infty} q^{n^2}\right)^2 =$$

$$= 1 + 4\left(\frac{q}{1-q} - \frac{q^3}{1-q^3} + \frac{q^5}{1-q^5} - \cdots\right). \tag{1}$$

今往證明：

定理 2. 若 $|q|<1$，則

$$q_0^4 q_2^8 = \left(\sum_{n=-\infty}^{\infty} q^{n^2}\right)^4 = 1 + 8\sum{}' \frac{mq^m}{1-q^m},$$

此處和號 $\sum'$ 過所有的非 4 之倍數之整數．換言之，

$$r_4(n) = 8\sum_{m|n}{}' m,$$

此處 m 乃 n 之因子但非 4 之倍數者．

在證明此定理時需要幾條預備定理．

命

$$u_r = \frac{q}{1-q^r},$$

則

$$\frac{q^r}{(1-q^r)^2} = u_r(1+u_r). \tag{2}$$

定理 3. $\sum_{m=1}^{\infty} u_m(1+u_m) = \sum_{n=1}^{\infty} nu_n.$

證： 由 (2) 式可知

$$\sum_{m=1}^{\infty} u_m(1+u_m) = \sum_{m=1}^{\infty} \frac{q^m}{(1-q^m)^2} = \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} nq^{mn} = \sum_{n=1}^{\infty} nu_n.$$

定理 4.

$$\sum_{m=1}^{\infty}(-1)^{m-1}u_{2m}(1+u_{2m}) = \sum_{n=1}^{\infty}(2n-1)u_{4n-2}.$$

證: 由 (2) 式可知

$$\sum_{m=1}^{\infty}(-1)^{m-1}u_{2m}(1+u_{2m})=\sum_{m=1}^{\infty}(-1)^{m-1}\frac{q^{2m}}{(1-q^{2m})^2}=$$

$$=\sum_{m=1}^{\infty}(-1)^{m-1}\sum_{r=1}^{\infty}r\,q^{2mr}=$$

$$=\sum_{r=1}^{\infty}r\sum_{m=1}^{\infty}(-1)^{m-1}q^{2mr}=\sum_{r=1}^{\infty}\frac{rq^{2r}}{1+q^{2r}}=$$

$$=\sum_{r=1}^{\infty}\left(\frac{rq^{2r}}{1-q^{2r}}-\frac{2rq^{4r}}{1-q^{4r}}\right)=\sum_{n=1}^{\infty}\frac{(2n-1)\,q^{4n-2}}{1-q^{4n-2}}.$$

定理 5. 若 θ 是一實數而非 π 之偶數倍,則

$$\left(\frac{1}{4}\cot\frac{1}{2}\theta+u_1\sin\theta+u_2\sin 2\theta+\cdots\right)^2=$$

$$=\left(\frac{1}{4}\cot\frac{1}{2}\theta\right)^2+C_0+\sum_{k=1}^{\infty}C_k\cos k\theta, \tag{3}$$

此處

$$C_0=\frac{1}{2}\sum_{n=1}^{\infty}n\,u_n,$$

$$C_k=u_k\left(1+u_k-\frac{1}{2}k\right),\qquad k\geqslant 1.$$

證: (3) 式之左邊等於

$$\left(\frac{1}{4}\cot\frac{1}{2}\theta\right)^2+\frac{1}{2}\sum_{n=1}^{\infty}u_n\cot\frac{1}{2}\theta\sin n\theta+$$

$$+\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}u_m u_n\sin m\theta\sin n\theta.$$

由

$$\frac{1}{2}\cot\frac{1}{2}\theta\sin n\theta=\frac{1}{2}+\cos\theta+\cdots+\cos(n-1)\theta+\frac{1}{2}\cos n\theta,$$

$$2\sin m\theta\sin n\theta=\cos(m-n)\theta-\cos(m+n)\theta,$$

可知該式等於

$$\left(\frac{1}{4}\cot\frac{1}{2}\theta\right)^2+\sum_{n=1}^{\infty}u_n\left(\frac{1}{2}+\cos\theta+\cdots+\cos(n-1)\theta+\frac{1}{2}\cos n\theta\right)+$$

$$+\frac{1}{2}\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}u_m u_n(\cos(m-n)\theta-\cos(m+n)\theta).$$

由此得出

$$C_0=\frac{1}{2}\sum_{n=1}^{\infty}(u_n+u_n^2),$$

$$C_k=\frac{1}{2}u_k+\sum_{n=k+1}^{\infty}u_n+$$

$$+\frac{1}{2}\sum_{m-n=k}u_m u_n+\frac{1}{2}\sum_{n-m=k}u_m u_n-\frac{1}{2}\sum_{n+m=k}u_m u_n,$$

此處 $m\geqslant 1,\ n\geqslant 1$.

由定理 3 可知

$$C_0=\frac{1}{2}\sum_{n=1}^{\infty}n u_n.$$

又

$$C_k=\frac{1}{2}u_k+\sum_{l=1}^{\infty}u_{k+l}+\sum_{l=1}^{\infty}u_l u_{k+l}-\frac{1}{2}\sum_{l=1}^{k-1}u_l u_{k-l}.$$

因爲

$$u_l u_{k-l}=u_k(1+u_l+u_{k-l})$$

及

$$u_{k+l}+u_l u_{k+l}=u_k(u_l-u_{k+l}),$$

所以

$$C_k=u_k\Big(\frac{1}{2}+\sum_{l=1}^{\infty}(u_l-u_{k+l})-\frac{1}{2}\sum_{l=1}^{k-1}(1+u_l+u_{k-l})\Big)=$$

$$=u_k\Big(\frac{1}{2}+u_1+\cdots+u_k-\frac{1}{2}(k-1)-(u_1+\cdots+u_{k-1})\Big)=$$

$$=u_k\Big(1+u_k-\frac{1}{2}k\Big).$$

定理 6.

$$\Big(\frac{1}{4}+\sum_{n=0}^{\infty}u_{4n+1}-\sum_{n=0}^{\infty}u_{4n+3}\Big)^2=\frac{1}{16}+\frac{1}{2}\sum_{\substack{m=1\\ 4\nmid m}}^{\infty}mu_m.$$

證：在定理 5 中取 $\theta=\frac{1}{2}\pi$，則得

$$\Big(\frac{1}{4}+\sum_{n=0}^{\infty}u_{4n+1}-\sum_{n=0}^{\infty}u_{4n+3}\Big)^2=$$

$$=\frac{1}{16}+\frac{1}{2}\sum_{n=1}^{\infty} n\, u_n+\sum_{m=1}^{\infty}(-1)^m C_{2m}=$$

$$=\frac{1}{16}+\frac{1}{2}\sum_{n=1}^{\infty} n\, u_n+\sum_{m=1}^{\infty}(-1)^m u_{2m}(1+u_{2m}-m)=$$

$$=\frac{1}{16}+\frac{1}{2}\sum_{m=1}^{\infty}(2m-1)\, u_{2m-1}+\sum_{m=1}^{\infty}(-1)^m u_{2m}(1+u_{2m})+$$

$$+2\sum_{m=1}^{\infty}(2m-1)\, u_{4m-2}=$$

$$=\frac{1}{16}+\frac{1}{2}\sum_{m=1}^{\infty}(2m-1)\, u_{2m-1}+\sum_{m=1}^{\infty}(2m-1)\, u_{4m-2}= \qquad \text{(由定理 4)}$$

$$=\frac{1}{16}+\frac{1}{2}\sum_{\substack{n=1\\ 4\nmid n}}^{\infty} n\, u_n .$$

定理 2 極易由定理 1 及定理 6 推得.

由定理 2 立刻可推得:

定理 7. $\frac{r_4(n)}{8}$ 是一積性函數.

定理 8 (Lagrange). 任一正整數可以表爲四個平方數之和.

此外還有以下之應用:

定理 9 (Jacobi). 有等式

$$q_2^8-q_3^8=16\, q\, q_1^8.$$

如以 §1 之表示代入,則得

$$\left(\prod_{n=1}^{\infty}(1+q^{2n-1})\right)^8-\left(\prod_{n=1}^{\infty}(1-q^{2n-1})\right)^8=16\, q\left(\prod_{n=1}^{\infty}(1+q^{2n})\right)^8.$$

(此結果 Jacobi 稱之爲 Aequatro identica ratis abstrura.)

證: 此式之兩邊同以 q_0^4 乘之,則由

$$(q_0\, q_2^2)^4=\left(\sum_{n=-\infty}^{\infty} q^{n^2}\right)^4=\sum_{n=0}^{\infty} r_4(n)\, q^n,$$

$$(q_0\, q_3^2)^4=\sum_{n=0}^{\infty} r_4(n)\,(-1)^n q^n$$

及

$$(2q_0 q_1^2)^4 = \left(\sum_{n=-\infty}^{\infty} q^{n(n+1)}\right)^4,$$

可知所求證之式與

$$q\left(\sum_{n=-\infty}^{\infty} q^{n(n+1)}\right)^4 = 2\sum_{\substack{n=0\\2\nmid n}}^{\infty} r_4(n)q^n$$

等價.

命 $s_4(n)$ 表

$$x_1(x_1+1)+\cdots+x_4(x_4+1)+1=n \tag{4}$$

之解數,此 n 必爲奇數. 故本定理有其數論上之意義; 即若 n 是一奇數,則 $s_4(n)$ 等於 $2r_4(n)$.

(4) 式乘 4, 並湊成平方,則得

$$(2x_1+1)^2+\cdots+(2x_4+1)^2=4n.$$

不定方程

$$y_1^2+y_2^2+y_3^2+y_4^2=4n$$

之 $r_4(4n)$ 個解只有二種: (i) y_1, y_2, y_3, y_4 全爲奇數, (ii) y_1, y_2, y_3, y_4 全爲偶數,由此可見

$$s_4(n)=r_4(4n)-r_4(n).$$

由定理 2, 可知

$$r_4(4n)=8\sum_{m|2n} m = 8\sum_{m|n}(m+2m)=3\left(8\sum_{m|n} m\right)=3r_4(n),$$

即

$$s_4(n)=2r_4(n).$$

故得定理.

習題 1. 經由以下之辦法算出

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots=\frac{\pi^2}{6}.$$

由四維空間球

$$u^2+v^2+w^2+z^2\leqslant x$$

中之整點數 $A(x)$ 之漸近公式

$$A(x)=\frac{\pi^2}{2}x^2+O\left(x^{\frac{3}{2}}\right),$$

並用定理 2 以求出另一表法．比較之而得習題中所求．

附註：由本習題及 (6.13.2) 立刻得到 $\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}=\frac{6}{\pi^2}$．

習題 2. 算出

$$\left(\frac{1}{6}+\frac{x}{1-x}-\frac{x^2}{1-x^2}+\frac{x^4}{1-x^4}-\frac{x^5}{1-x^5}+\cdots\right)^2=$$
$$=\frac{1}{36}+\frac{1}{3}\left(\frac{x}{1-x}+\frac{2x^2}{1-x^2}+\frac{4x^4}{1-x^4}+\frac{5x^5}{1-x^5}+\cdots\right).$$

習題 3. 利用

$$(1-\cos n\theta)\cot^2\frac{1}{2}\theta=(2n-1)+4(n-1)\cos\theta+4(n-2)\cos 2\theta+\cdots+$$
$$+4\cos(n-1)\theta+\cos n\theta$$

以證明

$$\left\{\frac{1}{8}\cot^2\frac{1}{2}\theta+\frac{1}{12}+\frac{x}{1-x}(1-\cos\theta)+\frac{2x^2}{1-x^2}(1-\cos 2\theta)+\right.$$
$$\left.+\frac{3x^3}{1-x^3}(1-\cos 3\theta)+\cdots\right\}^2=\left(\frac{1}{8}\cot^2\frac{1}{2}\theta+\frac{1}{12}\right)^2+$$
$$+\frac{1}{12}\left\{\frac{1^3x}{1-x}(5+\cos\theta)+\frac{2^3x^2}{1-x^2}(5+\cos 2\theta)+\right.$$
$$\left.+\frac{3^3x^3}{1-x^3}(5+\cos 3\theta)+\cdots\right\}.$$

§8. 密率.

命 $r_s(n,q)$ 表

$$x_1^2+\cdots+x_s^2\equiv n \pmod q \tag{1}$$

之解數．如將

$$x_1^2+\cdots+x_s^2=y$$

看成一變換，則左邊有 q^s 個值，而右邊有 q 個值．即對一個 y 之值，平均有 q^{s-1} 個解．今討論個別解數與平均解數之比值

$$\Delta_q(n)=\frac{r_s(n,q)}{q^{s-1}}.$$

又命

$$\partial_p(n)=\lim_{l\to\infty}\Delta_{p^l}(n),$$

此稱爲不定方程 (1) 之 p 密率.

又定義

$$\partial_0(n)=\lim_{\delta\to 0}\frac{1}{2\delta}\int\cdots\int_{n-\delta\leqslant x_1^2+\cdots+x_s^2\leqslant n+\delta}dx_1\cdots dx_s,$$

此稱爲 (1) 式之實密率.

今先往算出諸密率之值.

定理 1. 當 s 是偶數時,實密率等於

$$\frac{\pi^{s/2}}{\left(\frac{s}{2}-1\right)!}n^{\frac{s}{2}-1}. \tag{2}$$

證: 用極坐標可得積分

$$\iint_{1-x^2-y^2>0}(1-x^2-y^2)^{a-1}dxdy=\int_0^{2\pi}d\theta\int_0^1(1-\rho^2)^{a-1}\rho\,d\rho=\frac{\pi}{a}.$$

今往用歸納法證明:

$$V_s=\int\cdots\int_{1-x_1^2-\cdots-x_s^2>0}dx_1\cdots dx_s=\frac{\pi^{s/2}}{\left(\frac{s}{2}\right)!}.$$

命

$$x_\nu=y_{\nu-2}\sqrt{1-x_1^2-x_2^2},\qquad(\nu=3,\cdots,s).$$

則得

$$V_s=\iint_{1-x_1^2-x_2^2>0}(1-x_1^2-x_2^2)^{\frac{s-2}{2}}dx_1\,dx_2\int\cdots\int_{1-y_1^2-\cdots-y_{s-2}^2>0}dy_1\cdots dy_{s-2}=$$

$$=\frac{\pi}{\frac{s}{2}}V_{s-2}=\frac{\pi^{s/2}}{\left(\frac{s}{2}\right)!}.$$

由此得到

$$\partial_0(n)=\lim_{\delta\to 0}\frac{1}{2\delta}\left(\int\cdots\int_{x_1^2+\cdots+x_s^2\leqslant n+\delta}dx_1\cdots dx_s-\int\cdots\int_{x_1^2+\cdots+x_s^2\leqslant n-\delta}dx_1\cdots dx_s\right)=$$

$$=\frac{\pi^{s/2}}{\left(\frac{s}{2}\right)!}\lim_{\delta\to 0}\frac{(n+\delta)^{s/2}-(n-\delta)^{s/2}}{2\delta}=\frac{\pi^{s/2}}{\left(\frac{s}{2}-1\right)!}n^{\frac{s}{2}-1}.$$

要求出 p 密率，我們需要以下諸預備定理.

命

$$A_{p^l}(n)=\sum_{\substack{a=1\\ p\nmid a}}^{p^l}\frac{1}{p^{sl}}\left(\sum_{x=1}^{p^l}e^{2\pi iax^2/p^l}\right)^s e^{-2\pi ian/p^l}.$$

定理 2.

$$\sum_{m=0}^{l}A_{p^m}(n)=\Delta_{p^l}(n).$$

證:

$$\sum_{m=0}^{l}A_{p^m}(n)=\sum_{m=0}^{l}\sum_{\substack{a=1\\ p\nmid a}}^{p^m}\frac{1}{p^{sm}}\left(\sum_{x=1}^{p^m}e^{2\pi iax^2/p^m}\right)^s e^{-2\pi ian/p^m}=$$

$$=\sum_{m=0}^{l}\sum_{\substack{a=1\\ p^{l-m}\| a}}^{p^l}\frac{1}{p^{sl}}\left(\sum_{x=1}^{p^l}e^{2\pi iax^2/p^l}\right)^s e^{-2\pi ian/p^l}=$$

$$=\sum_{a=1}^{p^l}\frac{1}{p^{sl}}\left(\sum_{x=1}^{p^l}e^{2\pi iax^2/p^l}\right)^s e^{-2\pi ian/p^l}=$$

$$=\frac{1}{p^{(s-1)l}}\cdot\frac{1}{p^l}\sum_{a=1}^{p^l}\left(\sum_{x=1}^{p^l}e^{2\pi iax^2/p^l}\right)^s e^{-2\pi ian/p^l}=$$

$$=\frac{r_s(n,p^l)}{p^{(s-1)l}}=\Delta_{p^l}(n).$$

定理 3. 設 s 是 4 之倍數 $=4r$. 若 p 是奇素數, 則

$$A_{p^l}(n)=p^{-2rl}C_{p^l}(n).$$

證: 由定理 7.5.6 可知若 $p\nmid a$, 則

$$\left(\sum_{x=1}^{p^l}e^{2\pi iax^2/p^l}\right)^{4r}=p^{2rl},$$

故

$$A_{p^l}(n)=p^{-2rl}\sum_{\substack{a=1\\ p\nmid a}}^{p^l}e^{-2\pi ian/p^l}.$$

將 a 換為 $-a$ 卽得定理.

定理 4. 設 s 是 4 之倍數 $=4r$. 則

$$A_2(n)=0,$$

$$A_{2^l}(n) = (-1)^r 2^{-2r(l-1)} C_{2^l}(n).$$

證: 由定理 7.5.3 可知

$$A_2(n) = 0.$$

又由定理 7.5.7 可知,當 $2 \nmid a$ 時有

$$\sum_{x=1}^{2^l} e^{2\pi i a x^2/2^l} = \begin{cases} 2^{\frac{1}{2}l}(1+i^a), & \text{若 } 2 \mid l, \\ 2^{\frac{1}{2}(l+1)} e^{\frac{\pi i}{4}a}, & \text{若 } 2 \nmid l. \end{cases}$$

由於 $(1+i^a)^4 = -4$ 及 $\left(e^{\frac{\pi i}{4}a}\right)^4 = -1$, 故

$$\left(\sum_{x=1}^{2^l} e^{2\pi i a x^2/2^l}\right)^{4r} = (-1)^r 2^{2r(l+1)},$$

由此得出定理 4.

定理 5. 設 $s = 4r$, $p \neq 2$, $p^\tau \| n$, 則

$$\partial_p(n) = (1-p^{-2r}) \sum_{l=0}^{\tau} p^{-(2r-1)l} = (1-p^{-2r})(p^\tau)^{-(2r-1)} \sigma_{2r-1}(p^\tau),$$

此處

$$\sigma_t(n) = \sum_{d \mid n} d^t.$$

證: 由定理 3 及 7.4.4 可知

$$\partial_p(n) = \sum_{l=0}^{\infty} A_{p^l}(n) = 1 + \sum_{l=1}^{\infty} p^{-2rl} C_{p^l}(n) =$$

$$= 1 + \sum_{l=1}^{\tau} p^{-2rl}(p^l - p^{l-1}) - p^{-2r(\tau+1)} p^\tau =$$

$$= \sum_{l=0}^{\tau} p^{-2rl+l} - \sum_{l=1}^{\tau+1} p^{-2rl+l-1} =$$

$$= \sum_{l=0}^{\tau} p^{-(2r-1)l}(1-p^{-2r}).$$

定理 6. 設 $s = 4r$, 命 $2^\tau \| n$, 則

$$\partial_2(n) = \begin{cases} 1, & \text{若 } \tau = 0, \\ (1-2^{2-2r}+2^{(1-2r)(\tau+1)}(2^{2r}-1))(1-2^{1-2r})^{-1}, & \text{若 } \tau > 0, 2 \nmid r, \\ (1-2^{(1-2r)(\tau+1)}(2^{2r}-1))(1-2^{1-2r})^{-1}, & \text{若 } \tau > 0, 2 \mid r. \end{cases}$$

證明與定理 5 相仿,讀者自補足之.

定義. 命

$$\mathfrak{S}_s(n)=\prod_p \partial_p(n)$$

及

$$\delta_s(n)=\partial_0(n)\,\mathfrak{S}_s(n)=\partial_0(n)\prod_p \partial_p(n).$$

定理 7. 若 $s=4$, 則

$$\delta_4(n)=r_4(n)=8\sum_{\substack{d\mid n\\ 4\nmid d}} d.$$

證: 命 $n=2^\tau n'$, $2\nmid n'$, 則由 $\frac{1}{\zeta(s)}=\prod_p(1-p^{-s})$ 及定理 5 可知

$$\prod_{p>2}\partial_p(n)=\frac{4}{3}\,\frac{1}{\zeta(2)}\,n'^{-1}\sigma(n')=\frac{8}{\pi^2}\,n'^{-1}\sigma(n').$$

又由定理 1 可知

$$\partial_0(n)=\pi^2 n,$$

故

$$\partial_0(n)\prod_{p>2}\partial_p(n)=2^{\tau+3}\sigma(n').$$

若 n 是奇數,則已得定理. 若 n 是偶數,由定理 6 可知

$$\partial_2(n)=3\cdot 2^{-\tau}.$$

故得定理.

定理 8. 若 $s=8$, 則

$$\delta_8(n)=16(-1)^n\sum_{d\mid n}(-1)^d d^3.$$

證: 命 $n=2^\tau n'$, $2\nmid n'$, 則得

$$\prod_{p>2}\partial_p(n)=\frac{16}{15}\,\frac{1}{\zeta(4)}\,n'^{-3}\sigma_3(n')=$$

$$=\frac{96}{\pi^4}\,n'^{-3}\sigma_3(n').$$

又由定理 1,

$$\partial_0(n)=\frac{\pi^4}{6}n^3,$$

故得

$$\partial_0(n)\prod_{p>2}\partial_p(n)=16\cdot 2^{3\tau}\sigma_3(n').$$

又

$$\partial_2(n)=(1-2^{-3(\tau+1)}\cdot 15)\left(1-\frac{1}{8}\right)^{-1},$$

故

$$\delta_8(n)=16\cdot\frac{8}{7}\left(2^{3\tau}-\frac{15}{8}\right)\sigma_3(n').$$

當 n 是偶數時

$$\sum_{d\mid n}(-1)^d d^3=-\sigma_3(n')+2^3\sigma_3(n')+$$

$$+2^{3\cdot 2}\sigma_3(n')+\cdots+2^{3\cdot\tau}\sigma_3(n')=$$

$$=-2\sigma_3(n')+\frac{2^{3(\tau+1)}-1}{2^3-1}\sigma_3(n')=$$

$$=\left(-2+\frac{2^{3(\tau+1)}-1}{2^3-1}\right)\sigma_3(n')=$$

$$=\frac{8}{7}\left(2^{3\tau}-\frac{15}{8}\right)\sigma_3(n').$$

故得定理.

習題 1. 命 $s=2r$. 若 r 是偶數，則

$$(1-2^{-r})\zeta(r)\mathfrak{S}_s(2^\tau n')=$$

$$=\begin{cases} n'^{1-r}\sigma_{r-1}(n'), & \text{若 } \tau=0,\\ (1-2^{2-r}+2^{(1-r)(\tau+1)}(2^r-1))(1-2^{1-r})^{-1}n'^{1-r}\sigma_{r-1}(n'), & \text{若 } \tau>0,\ 2\parallel r,\\ (1-2^{(1-r)(\tau+1)}(2^r-1))(1-2^{1-r})^{-1}n'^{1-r}\sigma_{r-1}(n'), & \text{若 } \tau>0,\ 4\mid r.\end{cases}$$

若 r 是奇數，則

$$L(r)\mathfrak{S}_s(2^\tau n')=\left(\left(\frac{-1}{n}\right)+\left(\frac{-1}{r}\right)2^{(1-r)(\tau+1)}\right)n'^{1-r}\rho_{r-1}(n'),$$

此處

$$L(r)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^r},$$

而 $\chi(n)=0,\ 1,\ 0,\ -1$，當 $n\equiv 0,1,2,3 \pmod 4$. 又

$$\rho_t(n)=\sum_{q\mid n}\left(\frac{-1}{q}\right)q^t.$$

習題 2. 證明

$$\delta_2(n) = 2r_2(n).$$

習題 3. 證明

$$\delta_6(n) = 16\sum_{d \mid n} \chi\left(\frac{n}{d}\right) d^2 - 4\sum_{d \mid n} \chi(d)\, d^2.$$

§9. 關於平方和問題之總結.

上節已證明 $r_4(n) = \delta_4(n)$，此是否是一偶然之巧合？事實上，吾人可證明當 $3 \leqslant s \leqslant 8$ 時，常有

$$r_s(n) = \delta_s(n).$$

但當 $s > 8$ 時，此推測不再眞實.

迄今爲止，當 $s \leqslant 24$ 時，$r_s(n)$ 之公式皆已具體得出. 例如：

$$r_3(n) = \frac{16}{\pi} n^{\frac{1}{2}} \chi_2(n) K(-4n) \prod_{p^2 \mid n} \left(1 + \frac{1}{p} + \cdots + \frac{1}{p^{\tau-1}} + \right.$$

$$\left. + \frac{1}{p^{\tau}}\left(1 - \left(\frac{-p^{-2\tau} n}{p}\right) \frac{1}{p}\right)^{-1}\right),$$

此處 τ 之定義是 $p^{2\tau} \mid n$, $p^{2(\tau+1)} \nmid n$,

$$K(-4n) = \sum_{m=1}^{\infty} \left(\frac{-4n}{m}\right) \frac{1}{m},$$

又

$$\chi_2(n) = \begin{cases} 0, & 若\ 4^{-a} n \equiv 7 \pmod 8, \\ 2^{-a}, & 若\ 4^{-a} n \equiv 3 \pmod 8, \\ 3 \cdot 2^{-1-a}, & 若\ 4^{-a} n \equiv 1, 2, 5, 6 \pmod 8, \end{cases}$$

其中 a 之定義是 $4^a \mid n$, $4^{a+1} \nmid n$.

$$r_{24}(n) = \frac{16}{691} \sigma_{11}^{*}(n) + \frac{128}{691}\left((-1)^{n-1} 259\, \tau(n) - 512\, \tau\left(\frac{1}{2} n\right)\right),$$

此處

$$\sigma_{11}^{*}(n) = \sum_{d \mid n} (-1)^d d^{11},$$

而 $\tau(n)$ 是以下的冪級數

$$q\left((1-q)(1-q^2)\cdots\right)^{24} = \sum_{n=1}^{\infty} \tau(n)\, q^n$$

之係數，又若 $\frac{1}{2}n$ 非整數，則命 $\tau\left(\frac{1}{2}n\right)=0$.

由定理 3.6 可知

$$((1-q)(1-q^2)(1-q^3)\cdots)^3=\sum_{n=0}^{\infty}(-1)^n(2n+1)q^{\frac{1}{2}n(n+1)},$$

故

$$\tau(n)=\sum_{\frac{1}{2}x_1(x_1+1)+\cdots+\frac{1}{2}x_8(x_8+1)=n-1}((-1)^{x_1}(2x_1+1)+\cdots+(-1)^{x_8}(2x_8+1))=$$

$$=\sum_{\substack{y_1^2+\cdots+y_8^2=8n\\ 2\nmid y_1\cdots y_8}}\sum_{i=1}^{8}(-1)^{\frac{1}{2}(y_i-1)}y_i.$$

具體算出者人名如下表:

s	$r_s(n)$ 之求出者
2, 4, 6, 8	Jacobi, 1828
3	Dirichlet
5, 7	Eisenstein, Smith, Minkowski
10, 12	Liouville, 1864, 1866
14, 16, 18	Glaisher, 1907
20, 22, 24	Ramanujan, 1916
9, 11, 13 15, 17, 19 21, 23	Ломадзе, 1949

第　九　章

素　數　定　理

§1. 引言. 本章之主要目的在於證明下式:

$$\pi(x) \sim \frac{x}{\log x}, \tag{1}$$

此處 $\pi(x)$ 代表不大於 x 的素數的個數. (1) 式卽爲著名的素數定理. 本章將給出兩個證明: 其一應用了比較高深的分析知識 (讀者需具有一定程度的高等微積分及複變數函數論的知識), 但比較直覺一些, 其基本思路是 N. Wiener 所首創者. 另一證明雖然並不用到很多分析學上的知識, 可以認爲是一個初等證明, 但却比較難懂. 此一證明是 Erdös 及 Selberg 所發明的. 關於尋求素數定理之"初等證明", 乃素數論中歷時很久的難題之一,此證明之獲得乃 1949 年之事也.

在以下各節中,我們並不直接去證明 (1) 式, 而證明另外二個與 (1) 式貌異實同的定理.

設 $x>0$. 令

$$\vartheta(x) = \sum_{p \leqslant x} \log p, \tag{2}$$

$$\psi(x) = \sum_{n \leqslant x} \Lambda(n) = \sum_{p^m \leqslant x} \log p. \tag{3}$$

(3) 式中的 $\Lambda(n)$ 卽爲 §6.1 例 6 中的 Von Mangoldt 函數. $\vartheta(x)$, $\psi(x)$ 稱爲 Чебышев 函數. 容易得到

$$\psi(x) = \vartheta(x) + \vartheta(x^{1/2}) + \vartheta(x^{1/3}) + \cdots \tag{4}$$

及

$$\psi(x) = \sum_{p \leqslant x} \left[\frac{\log x}{\log p}\right] \log p, \tag{5}$$

式中$\left[\frac{\log x}{\log p}\right]$表示$\frac{\log x}{\log p}$的整數部分.

定理 1. 我們有

$$\overline{\lim_{x\to\infty}}\frac{\pi(x)}{x(\log x)^{-1}}=\overline{\lim_{x\to\infty}}\frac{\vartheta(x)}{x}=\overline{\lim_{x\to\infty}}\frac{\psi(x)}{x}\tag{6}$$

及

$$\underline{\lim_{x\to\infty}}\frac{\pi(x)}{x(\log x)^{-1}}=\underline{\lim_{x\to\infty}}\frac{\vartheta(x)}{x}=\underline{\lim_{x\to\infty}}\frac{\psi(x)}{x}.\tag{7}$$

證: 由 (4) 及 (5) 易得

$$\vartheta(x)\leqslant\psi(x)\leqslant\sum_{p\leqslant x}\frac{\log x}{\log p}\log p=\pi(x)\log x,$$

故

$$\overline{\lim_{x\to\infty}}\frac{\vartheta(x)}{x}\leqslant\overline{\lim_{x\to\infty}}\frac{\psi(x)}{x}\leqslant\overline{\lim_{x\to\infty}}\frac{\pi(x)}{x(\log x)^{-1}}.$$

又設 $0<\alpha<1$, $x>1$, 則

$$\vartheta(x)\geqslant\sum_{x^{\alpha}<p\leqslant x}\log p\geqslant\left\{\pi(x)-\pi(x^{\alpha})\right\}\log x^{\alpha}\geqslant$$

$$\geqslant\alpha\left\{\pi(x)-x^{\alpha}\right\}\log x.$$

因爲 $\lim\limits_{x\to\infty}\frac{\log x}{x^{1-\alpha}}=0$, 故

$$\overline{\lim_{x\to\infty}}\frac{\vartheta(x)}{x}\geqslant\alpha\,\overline{\lim_{x\to\infty}}\frac{\pi(x)}{x(\log x)^{-1}}$$

對於任何小於 1 的正數 α 成立. 故得

$$\overline{\lim_{x\to\infty}}\frac{\vartheta(x)}{x}\geqslant\overline{\lim_{x\to\infty}}\frac{\pi(x)}{x(\log x)^{-1}}.$$

聯合前面已得到的結果,故

$$\overline{\lim_{x\to\infty}}\frac{\pi(x)}{x(\log x)^{-1}}=\overline{\lim_{x\to\infty}}\frac{\vartheta(x)}{x}=\overline{\lim_{x\to\infty}}\frac{\psi(x)}{x}.$$

至於 (7) 式,亦可以同樣證明之.

由定理 1 及定理 5.6.2 立得

定理 2. 設 $x\geqslant2$, 則存在常數 $c_i>0$ $(i=1,2,3,4)$, 使

$$c_1x\leqslant\vartheta(x)\leqslant c_2x,\tag{8}$$

及

$$c_3 x \leqslant \psi(x) \leqslant c_4 x \tag{9}$$

成立.

又由定理 1 立刻看到,若欲證明 (1) 式,祇需證明

$$\psi(x) \sim x \tag{10}$$

或

$$\vartheta(x) \sim x. \tag{11}$$

在證明 (10) 式之前,先來敍述若干必要的預備知識.

§ 2. Riemann ζ 函數.

今後常用 $s = \sigma + it$ 表一複數, σ 及 t 爲實數,級數

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad (\sigma > 1) \tag{1}$$

稱爲 Riemann ζ 函數.

給一 $a > 1$, 當 $\sigma \geqslant a$ 時,因爲

$$\left| \sum_{n=N}^{\infty} \frac{1}{n^s} \right| \leqslant \sum_{n=N}^{\infty} \frac{1}{n^\sigma} \leqslant \sum_{n=N}^{\infty} \frac{1}{n^a},$$

故 $\zeta(s)$ 當 $\sigma \geqslant a > 1$ 時是一致收斂的. 由於 a 是大於 1 的任意正數,故 $\zeta(s)$ 在 $\sigma > 1$ 的半平面上是一個正則函數.

定理 1. 命

$$h(s) = \zeta(s) - \frac{1}{s-1}.$$

在半平面 $\sigma > 0$ 上, $h(s)$ 是正則函數,且

$$|h(s)| \leqslant \frac{|s|}{\sigma} \quad (\sigma > 0).$$

證: 命

$$f_n(s) = n^{-s} - \int_n^{n+1} u^{-s}\, du,$$

則

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \sum_{n=1}^{\infty} f_n(s) + \int_1^{\infty} u^{-s}\, du = \sum_{n=1}^{\infty} f_n(s) + \frac{1}{s-1} \quad (\sigma > 1). \tag{2}$$

因

$$|n^{-s}-u^{-s}|=\left|\int_n^u sv^{-s-1}\,dv\right|\leqslant|s|\int_n^{n+1}v^{-\sigma-1}\,dv\quad(n\leqslant u\leqslant n+1),$$

故

$$|f_n(s)|=\left|\int_n^{n+1}(n^{-s}-u^{-s})\,du\right|\leqslant|s|\int_n^{n+1}v^{-\sigma-1}\,dv.$$

設 $0<a\leqslant\sigma\leqslant b$, $-T\leqslant t\leqslant T$, 則

$$\left|\sum_{n=N}^{\infty}f_n(s)\right|\leqslant\sum_{n=N}^{\infty}|f_n(s)|\leqslant|s|\int_N^{\infty}v^{-\sigma-1}\,dv=\frac{|s|}{\sigma}N^{-\sigma}\leqslant$$
$$\leqslant\frac{\sqrt{b^2+T^2}}{a}N^{-a},$$

故級數 $\sum_{n=1}^{\infty}f_n(s)$ 在 $0<a\leqslant\sigma\leqslant b$, $-T\leqslant t\leqslant T$ 內一致收斂. 由於 a 可以任意接近於 0, 而 b, T 可以任意大, 故 $h(s)=\sum_{n=1}^{\infty}f_n(s)$ 在 $\sigma>0$ 之半平面上是正則函數. 因此 (2) 式可以看作 $\zeta(s)$ 在半平面 $\sigma>0$ 上的解析開拓, 而 $s=1$ 爲其僅有的一次極, 且留數爲 1.

由 (2) 式卽得

$$\left|\zeta(s)-\frac{1}{s-1}\right|=\left|\sum_{n=1}^{\infty}f_n(s)\right|\leqslant|s|\int_1^{\infty}v^{-\sigma-1}\,dv=\frac{|s|}{\sigma}\quad(\sigma>0).$$

定理證完.

定理 2. 在半平面 $\sigma\geqslant1$ 上, $\zeta(s)\neq0$.

證: 當 $\sigma>1$ 時, $\sum_{n=1}^{\infty}\frac{1}{n^s}$ 絕對收斂, 故由定理 5.4.4 得到

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_p(1-p^{-s})^{-1},\tag{3}$$

此處連乘積過所有的素數 p. 由於每一因子皆非零, 而乘積又絕對收斂, 故當 $\sigma>1$ 時, $\zeta(s)\neq0$.

在 $s=1$ 時, $\zeta(s)$ 有一次極, 今需證明者爲: 當 $t\neq0$ 時,

$$\zeta(1+it)\neq0.$$

今研究函數

$$\varphi_\varepsilon(t)=|\zeta(1+\varepsilon)|^3|\zeta(1+\varepsilon+it)|^4|\zeta(1+\varepsilon+2it)|$$

$(\varepsilon>0,\ t\neq0)$. 由 (3) 可知

$$\varphi_\varepsilon(t)=\prod_p a_p,$$

此處

$$a_p=\left|1-\frac{1}{p^{1+\varepsilon}}\right|^{-3}\cdot\left|1-\frac{1}{p^{1+\varepsilon+it}}\right|^{-4}\cdot\left|1-\frac{1}{p^{1+\varepsilon+2it}}\right|^{-1},$$

故

$$\log a_p=-3\log\left(1-\frac{1}{p^{1+\varepsilon}}\right)-4R\log\left(1-\frac{1}{p^{1+\varepsilon+it}}\right)-R\log\left(1-\frac{1}{p^{1+\varepsilon+2it}}\right)=$$

$$=\sum_{m=1}^{\infty}\frac{1}{m}p^{-(1+\varepsilon)m}(3+4\cos(mt\log p)+\cos(2mt\log p)).$$

由於 $3+4\cos\theta+\cos 2\theta=2(1+\cos\theta)^2\geqslant 0$，故得

$$\log a_p\geqslant 0,$$

卽

$$|\varphi_\varepsilon(t)|\geqslant 1. \tag{4}$$

若 $\zeta(1+it)=0$，則

$$\zeta(1+\varepsilon+it)=\int_1^{1+\varepsilon}\zeta'(\sigma+it)\,d\sigma=O(\varepsilon).$$

由定理 1 已知

$$\varepsilon\zeta(1+\varepsilon)=O(1),$$

故可得，對任意小的 ε，常有

$$\varphi_\varepsilon(t)=O(\varepsilon),$$

此與 (4) 式相矛盾.

定理 3. 命

$$\frac{\zeta'(s)}{\zeta(s)}+\frac{1}{s-1}=g(s).$$

當 $\sigma\geqslant 1$，$g(s)$ 有一級連續導數.

證：微分定理 1 中之 $h(s)$，可得

$$\zeta'(s)=-\frac{1}{(s-1)^2}+h'(s),$$

此處 $h'(s)$ 是在半平面 $\sigma>0$ 上有處處連續導數的函數. 再則，由定理 2 可知

$$\frac{1}{\zeta(s)}=\frac{s-1}{1+(s-1)h(s)}$$

在 $\sigma\geqslant 1$ 的半平面上正則，故在此半平面上 $1+(s-1)h(s)\neq 0$.

因此，

$$\frac{\zeta'(s)}{\zeta(s)} = \frac{-\left(\frac{1}{(s-1)^2} - h'(s)\right)(s-1)}{1+(s-1)h(s)} =$$

$$= -\frac{1}{s-1} + g(s),$$

此 $g(s)$ 適合定理中所要求的性質.

§3. 若干引理.

定理 1. 若 $f(x)$ 有一級連續導數，則

$$\int_a^b f(x)\,e^{ixt}\,dx = O\left(\frac{1}{t}\right). \tag{1}$$

證： 用分部積分法可知

$$\int_a^b f(x)\,e^{ixt}\,dx = \frac{1}{it}\left\{\left[f(x)\,e^{ixt}\right]_a^b - \int_a^b f'(x)\,e^{ixt}\,dx\right\} = O\left(\frac{1}{t}\right).$$

定理 2.

$$\int_{-\infty}^{\infty} \frac{\sin x}{x}\,dx = \pi. \tag{2}$$

證： 命

$$J = \int_0^\infty e^{-kx}\,\frac{\sin \alpha x}{x}\,dx \qquad (1 \leqslant \alpha \leqslant 2,\quad 0 \leqslant k \leqslant 1).$$

固定 $k > 0$，被積分函數是 α 及 x 的連續函數，其關於 α 之偏導數爲 $e^{-kx}\cos \alpha x$，亦爲 x 及 α 之連續函數. 由於

$$\int_0^\infty e^{-kx}\,dx$$

存在， 故積分

$$\int_0^\infty e^{-kx}\cos \alpha x\,dx$$

關於 $1 \leqslant \alpha \leqslant 2$ 一致收斂. 因此關於 J 可以在積分號下求微分，即

$$\frac{dJ}{d\alpha} = \int_0^\infty e^{-kx}\cos \alpha x dx = \frac{k}{\alpha^2+k^2}.$$

此等式之右邊連用二次分部積分卽得. 再積分上式得

$$J = \tan^{-1}\frac{\alpha}{k} \qquad (1 \leqslant \alpha \leqslant 2,\qquad 0 < k \leqslant 1).$$

固定 α, 當 $0 \leqslant k \leqslant 1$ 時, J 是一致收斂的, 故 J 當 $0 \leqslant k \leqslant 1$ 連續. 因此

$$\lim_{k\to 0+} J = \int_0^\infty \frac{\sin \alpha x}{x}\, dx = \lim_{k\to 0+} \tan^{-1}\frac{\alpha}{k} = \frac{\pi}{2}.$$

特別當 $\alpha = 1$ 時,

$$\int_{-\infty}^\infty \frac{\sin x}{x}\, dx = 2\int_0^\infty \frac{\sin x}{x}\, dx = \pi.$$

定理 3. 命 $a < 0 < b$. 若 $f(x)$ 有二級連續導數,則

$$\lim_{\omega\to\infty} \frac{1}{\pi}\int_a^b f(x)\frac{\sin \omega x}{x}\, dx = f(0). \tag{3}$$

證: 今研究

$$\int_a^b (f(x) - f(0))\frac{\sin \omega x}{x}\, dx.$$

在 0 點 $\frac{1}{x}(f(x) - f(0))$ 有一級連續導數,故由定理 1 可知

$$\lim_{\omega\to\infty} \int_a^b (f(x) - f(0))\frac{\sin \omega x}{x}\, dx = 0,$$

即

$$\lim_{\omega\to\infty} \frac{1}{\pi}\int_a^b f(x)\frac{\sin \omega x}{x}\, dx = f(0)\lim_{\omega\to\infty}\frac{1}{\pi}\int_a^b \frac{\sin \omega x}{x}\, dx =$$

$$= f(0)\frac{1}{\pi}\lim_{\omega\to\infty}\int_{a\omega}^{b\omega}\frac{\sin x}{x}\, dx = f(0)\frac{1}{\pi}\int_{-\infty}^\infty \frac{\sin x}{x}\, dx.$$

由定理 2 即得定理.

定理 4. 命 $\lambda > 0$ 及

$$K_\lambda(x) = \begin{cases} 1 - \dfrac{|x|}{2\lambda}, & 若\ |x| \leqslant 2\lambda, \\ 0, & 若\ |x| > 2\lambda. \end{cases}$$

則得

$$\frac{1}{\sqrt{2\pi}}\int_{-\infty}^\infty K_\lambda(t)\, e^{ixt}\, dt = k_\lambda(x), \tag{4}$$

此處

$$k_\lambda(x) = \begin{cases} \dfrac{2\lambda}{\sqrt{2\pi}}\left(\dfrac{\sin \lambda x}{\lambda x}\right)^2, & 若\ x \neq 0, \\ \dfrac{2\lambda}{\sqrt{2\pi}}, & 若\ x = 0. \end{cases}$$

證: 易見

$$k_\lambda(x) = \frac{2}{\sqrt{2\pi}} \int_0^{2\lambda} \left(1 - \frac{t}{2\lambda}\right) \cos xt \, dt. \tag{5}$$

若 $x = 0$, 顯見

$$k_\lambda(x) = \frac{1}{\sqrt{2\pi}} 2\lambda.$$

若 $x \neq 0$, 用分部積分法卽得所求.

定理 5.

$$K_\lambda(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} k_\lambda(t) \, e^{ixt} \, dt. \tag{6}$$

特別取 $\lambda = 1$, $x = 0$, 可得

$$\frac{1}{\pi} \int_{-\infty}^{\infty} \frac{\sin^2 x}{x^2} \, dx = 1. \tag{7}$$

證: 先研究積分

$$I(\omega) = \frac{1}{\sqrt{2\pi}} \int_{-\omega}^{\omega} k_\lambda(t) \, e^{ixt} \, dt = \frac{2}{\sqrt{2\pi}} \int_0^{\omega} k_\lambda(t) \cos xt \, dt.$$

由 (5) 可知

$$I(\omega) = \frac{2}{\pi} \int_0^{\omega} \int_0^{2\lambda} \left(1 - \frac{u}{2\lambda}\right) \cos ut \cos xt \, du dt =$$

$$= \frac{1}{\pi} \int_0^{2\lambda} \left(1 - \frac{u}{2\lambda}\right) du \int_0^{\omega} (\cos(u + x) t + \cos(u - x) t) \, dt =$$

$$= \frac{1}{\pi} \int_0^{2\lambda} \left(1 - \frac{u}{2\lambda}\right) \left(\frac{\sin(u+x)\omega}{u + x} + \frac{\sin(u-x)\omega}{u - x}\right) du.$$

若 $x > 2\lambda$, 由定理 1 可知 $\lim\limits_{\omega\to\infty} I(\omega) = 0$; 若 $0 < x < 2\lambda$, 則由定理 1 及定理 3 可知上式第一項之極限爲 0, 第二項之極限爲 $1 - \frac{x}{2\lambda}$. 由於積分 (6) 爲 x 之連續函數, 可知 $K_\lambda(2\lambda) = 0$, $K_\lambda(0) = 1$. 故得定理.

定理 6. 若 $f(t) \geqslant 0$ $(0 \leqslant t \leqslant \infty)$, 且對任一 $T > 0$, 區間 $0 \leqslant t \leqslant T$ 可以分爲有限段, 每一段中 $f(t)$ 都是連續的. 又設對任一 $\varepsilon > 0$, 積分

$$\int_0^{\infty} e^{-\varepsilon t} f(t) \, dt$$

收斂, 則

$$\lim_{\varepsilon\to 0} \int_0^{\infty} e^{-\varepsilon t} f(t) \, dt = \int_0^{\infty} f(t) \, dt. \tag{8}$$

證: 因 $f(t)\geqslant 0$, 故 $\int_0^T f(t)dt$ 隨 T 之增加而增加,因之

$$\int_0^\infty f(t)\,dt$$

或爲一有限數,或爲 ∞.

因

$$\int_0^\infty e^{-\varepsilon t} f(t)\,dt \leqslant \int_0^\infty f(t)\,dt,$$

故

$$\overline{\lim_{\varepsilon\to 0}} \int_0^\infty e^{-\varepsilon t} f(t)\,dt \leqslant \int_0^\infty f(t)\,dt.$$

但另一方面

$$\int_0^\infty e^{-\varepsilon t} f(t)\,dt \geqslant \int_0^T e^{-\varepsilon t} f(t)\,dt \geqslant e^{-\varepsilon T}\int_0^T f(t)\,dt,$$

故

$$\underline{\lim_{\varepsilon\to 0}} \int_0^\infty e^{-\varepsilon t} f(t)\,dt \geqslant \int_0^T f(t)\,dt.$$

命 $T\to\infty$, 立得

$$\underline{\lim_{\varepsilon\to 0}} \int_0^\infty e^{-\varepsilon t} f(t)\,dt \geqslant \int_0^\infty f(t)dt.$$

故得定理.

§4. Tauber 型定理.

定義. 若 $f(x)$ 在 $-\infty<x<\infty$ 中有定義,且適合

$$\underline{\lim_{\substack{y-x\to 0\\ x\to\infty}}}\{f(y)-f(x)\}\geqslant 0 \qquad (y>x), \tag{1}$$

則 $f(x)$ 稱爲慢遞減函數.

定理 1. 設 $f(x)$ 是慢遞減函數,且滿足 $|f(x)|<M$ $(-\infty<x<\infty)$. 若對於所有的 $\lambda>0$ 皆有

$$\lim_{x\to\infty}\frac{1}{\sqrt{2\pi}}\int_{-\infty}^\infty k_\lambda(x-t)\,f(t)\,dt=l,$$

則 $f(x)\to l$ $(x\to\infty)$.

證: 由定理 3.5 可知

$$\frac{1}{\sqrt{2\pi}}\int_{-\infty}^\infty k_\lambda(x-t)\,dt=\frac{1}{\pi}\int_{-\infty}^\infty \frac{\sin^2 u}{u^2}\,du=1,$$

故不失一般性,我們可以假定 $l=0$.

若 $f(x)\nrightarrow 0$, 則必存在 $\delta>0$ 及一數列 $\{x_n\}$ $(x_n\to\infty)$, 使 $f(x_n)<-\delta$ $(n=1,2,\cdots)$ 或 $f(x_n)>\delta$ 成立. 不失一般性, 吾人假定 $f(x_n)>\delta$ $(n=1,2,\cdots)$. ($f(x_n)<-\delta$ $(n=1,2,\cdots)$ 之情况同樣證之.)

因 $f(x)$ 爲慢遞減函數,故存在 $x_0=x_0(\delta)$ 及 $\eta=\eta(\delta)$, 使

$$f(y)-f(x)\geqslant-\frac{\delta}{2}\qquad(x\geqslant x_0,\quad 0\leqslant y-x\leqslant 2\eta)$$

成立. 特別取 $x\in\{x_n\}$, 則得

$$f(y)>\frac{\delta}{2}\quad(x_0\leqslant x\leqslant y\leqslant x+2\eta,\quad x\in\{x_n\}).\tag{2}$$

由 (2), 當 $x\geqslant x_0$ 及 $x\in\{x_n\}$ 時,

$$\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}k_\lambda(x+\eta-t)\,f(t)\,dt\geqslant$$

$$\geqslant\frac{\delta}{2\sqrt{2\pi}}\int_x^{x+2\eta}k_\lambda(x+\eta-t)\,dt-\frac{M}{\sqrt{2\pi}}\int_{-\infty}^{x}k_\lambda(x+\eta-t)\,dt-$$

$$-\frac{M}{\sqrt{2\pi}}\int_{x+2\eta}^{\infty}k_\lambda(x+\eta-t)dt=$$

$$=\frac{\delta}{2\sqrt{2\pi}}\int_{x-\eta}^{x+\eta}k_\lambda(x-u)\,du-\frac{M}{\sqrt{2\pi}}\int_{-\infty}^{x-\eta}k_\lambda(x-u)\,du-$$

$$-\frac{M}{\sqrt{2\pi}}\int_{x+\eta}^{\infty}k_\lambda(x-u)\,du=$$

$$=\frac{\delta}{\sqrt{2\pi}}\int_0^{\eta}k_\lambda(v)\,dv-\frac{2M}{\sqrt{2\pi}}\int_{\eta}^{\infty}k_\lambda(v)\,dv=$$

$$=\frac{\delta}{\pi}\int_0^{\lambda\eta}\frac{\sin^2 w}{w^2}\,dw-\frac{2M}{\pi}\int_{\lambda\eta}^{\infty}\frac{\sin^2 w}{w^2}\,dw$$

$$\longrightarrow\frac{\delta}{2}\,(\lambda\to\infty),$$

故存在 λ_0 適當大,使

$$\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}k_{\lambda_0}(x+\eta-t)\,f(t)\,dt>\frac{\delta}{4}\qquad(x\geqslant x_0,\quad x\in\{x_n\}).$$

命 x 按 $\{x_n\}$ 趨於無窮,則

$$\varlimsup_{\substack{x\to\infty \\ x\in\{x_n\}}} \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} k_{\lambda_0}(x+\eta-t)\,f(t)\,dt \geqslant \frac{\delta}{4},$$

與假設相矛盾. 故必須 $f(x)\to 0$. 定理證完.

定理 2 (Ikehara). 設 $h(t)$ 是區間 $0\leqslant t<\infty$ 上的非負遞增函數,且對有限數 T, 在區間 $0\leqslant t\leqslant T$ 中, $h(t)$ 祇有有限個不連續點; 又若積分

$$f(s)=\int_0^{\infty} e^{-st}\,h(t)\,dt \qquad (\sigma>1) \tag{3}$$

收斂,且對任何有限數 a, 有固定的常數 A, 使

$$\lim_{\sigma\to 1}\left(f(s)-\frac{A}{s-1}\right)=g(t) \tag{4}$$

在區間 $|t|\leqslant a$ 中一致成立,而 $g(t)$ 有一級連續導數,則

$$\lim_{t\to\infty} e^{-t}\,h(t)=A. \tag{5}$$

證: 命

$$a(t)=\begin{cases} e^{-t}\,h(t) & (t\geqslant 0),\\ 0 & (t<0);\end{cases} \qquad A(t)=\begin{cases} A & (t\geqslant 0),\\ 0 & (t<0).\end{cases}$$

今往證明以下諸事: 1) 對任何 $\lambda>0$, 積分

$$I_\lambda(x)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} k_\lambda(x-t)\,(a(t)-A(t))\,dt \tag{6}$$

存在; 2)

$$\lim_{x\to\infty} I_\lambda(x)=0 \tag{7}$$

及 3) $a(t)-A(t)$ 是有界慢遞減函數. 若此三點證明,則由定理 1 可得出本定理.

考慮積分

$$I_{\lambda,\varepsilon}(x)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} k_\lambda(x-t)\,(a(t)-A(t))\,e^{-\varepsilon t}\,dt.$$

由假定可知此積分對任意 $\varepsilon>0$, $\lambda>0$ 皆存在. 由定理 3.4 及因積分

$$\int_{-\infty}^{\infty} (a(t)-A(t))\,e^{-(\varepsilon+iy)t}\,dt$$

關於 $|y|\leqslant 2\lambda$ 是一致收斂的,故

$$I_{\lambda,\varepsilon}(x)=\frac{1}{2\pi}\int_{-\infty}^{\infty}(a(t)-A(t))\,e^{-\varepsilon t}\,dt\int_{-2\lambda}^{2\lambda}K_\lambda(y)\,e^{i(x-t)y}\,dy=$$

$$=\frac{1}{2\pi}\int_{-2\lambda}^{2\lambda}K_\lambda(y)\,e^{ixy}\,dy\int_{-\infty}^{\infty}(a(t)-A(t))\,e^{-(\varepsilon+iy)t}\,dt=$$

$$=\frac{1}{2\pi}\int_{-2\lambda}^{2\lambda}K_\lambda(y)\,e^{ixy}\left(f(1+\varepsilon+iy)-\frac{A}{\varepsilon+iy}\right)dy.$$

由 (4) 可知

$$\lim_{\varepsilon\to 0} I_{\lambda,\varepsilon}(x)=\frac{1}{2\pi}\int_{-2\lambda}^{2\lambda}g(y)\,K_\lambda(y)\,e^{ixy}\,dy\,. \tag{8}$$

再由定理 3.1 可知

$$\lim_{x\to\infty}\lim_{\varepsilon\to 0} I_{\lambda,\varepsilon}(x)=0\,. \tag{9}$$

但另一方面,由定理 3.6,

$$\lim_{\varepsilon\to 0} I_{\lambda,\varepsilon}(x)=\lim_{\varepsilon\to 0}\frac{1}{\sqrt{2\pi}}\left(\int_0^{\infty}k_\lambda(x-t)\,a(t)\,e^{-\varepsilon t}\,dt-A\int_0^{\infty}k_\lambda(x-t)\,e^{-\varepsilon t}\,dt\right)=$$

$$=\frac{1}{\sqrt{2\pi}}\int_0^{\infty}k_\lambda(x-t)\,a(t)\,dt-\frac{A}{\sqrt{2\pi}}\int_0^{\infty}k_\lambda(x-t)\,dt=$$

$$=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}k_\lambda(x-t)\,(a(t)-A(t))\,dt=I_\lambda(x)\,,$$

故由 (8) 式可知 $I_\lambda(x)$ 是存在的,卽得性質 1). 再由 (9) 式得性質 2).

今往證明性質 3). 由 $A(t)$ 之定義,可知祇需證明 $a(t)$ 是有界慢遞減函數卽可.

由 (7) 式,

$$\lim_{x\to\infty}\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}k_\lambda(x-t)\,a(t)\,dt=\lim_{x\to\infty}\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}k_\lambda(x-t)\,A(t)\,dt=$$

$$=\frac{A}{\sqrt{2\pi}}\lim_{x\to\infty}\int_{-\infty}^{\lambda x}\sqrt{\frac{2}{\pi}}\left(\frac{\sin u}{u}\right)^2du=$$

$$=\frac{A}{\pi}\int_{-\infty}^{\infty}\left(\frac{\sin u}{u}\right)^2du=A\,,$$

故存在 x_0, 當 $x\geqslant x_0$ 時,

$$\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}k_\lambda(x-t)\,a(t)\,dt<A+1\,,$$

卽

$$\int_{-\infty}^{\infty}\left(\frac{\sin t}{t}\right)^2 a\left(x-\frac{t}{\lambda}\right)dt < \pi(A+1) \qquad (x \geqslant x_0).$$

由於被積函數是非負的,並以 $x+\frac{2}{\sqrt{\lambda}}$ 代替 x, 可得

$$\int_{-\sqrt{\lambda}}^{\sqrt{\lambda}}\left(\frac{\sin t}{t}\right)^2 a\left(x+\frac{2}{\sqrt{\lambda}}-\frac{t}{\lambda}\right)dt < \pi(A+1) \qquad (x \geqslant x_0).$$

又由假定可知 $e^t a(t)$ 乃 t 之遞增函數,故

$$a(x)\, e^{-\frac{3}{\sqrt{\lambda}}}\int_{-\sqrt{\lambda}}^{\sqrt{\lambda}}\left(\frac{\sin t}{t}\right)^2 dt < \pi(A+1) \qquad (x \geqslant x_0).$$

命 $\lambda \to \infty$, 卽得

$$a(x) \leqslant A+1 \qquad (x \geqslant x_0).$$

當 $x < x_0$ 時, $h(x)$ 有界, 故 $a(x)$ 亦然, 此證明了 $a(x)$ 在 $-\infty < x < \infty$ 中是一有界函數.

又對任一 $\delta > 0$, 有

$$a(x+\delta)-a(x) = e^{-x}\{e^{-\delta} h(x+\delta) - h(x)\} \geqslant$$
$$\geqslant e^{-x} h(x)\,(e^{-\delta}-1),$$

故

$$\varliminf_{\substack{x\to\infty\\ \delta\to 0}}\{a(x+\delta)-a(x)\} \geqslant 0,$$

卽 $a(x)$ 是一慢遞減函數. 定理證完.

§5. 素數定理.

本節將應用 Ikehara 定理來證明素數定理. 吾人並不直接證明素數定理, 而去證明下面與素數定理貌異實同的定理 (參看 §1).

定 理 1. $\psi(x) \sim x$.

證: 由於 $\psi(x)$ 的定義可知 $\psi(x)$ 是 x 的非負遞增函數, 且對任意 T, 在區間 $0 \leqslant t \leqslant T$ 中祇有有限個不連續點.

當 $\sigma > 1$ 時, 由定理 1.2, 及 (6.14.5) 式得

$$\int_0^{\infty} e^{-st}\psi(e^t)\,dt = \int_1^{\infty} u^{-(1+s)}\psi(u)\,du =$$

$$= \sum_{n=1}^{\infty}\int_n^{n+1} u^{-(1+s)}\psi(u)\,du = \sum_{n=1}^{\infty}\sum_{m\leqslant n}\Lambda(m)\int_n^{n+1} u^{-(s+1)}du =$$

$$=\frac{1}{s}\sum_{n=1}^{\infty}(n^{-s}-(n+1)^{-s})\sum_{m\leqslant n}\Lambda(m)=\frac{1}{s}\lim_{N\to\infty}\sum_{n=1}^{N}(n^{-s}-(n+1)^{-s})\sum_{m\leqslant n}\Lambda(m)=$$

$$=\frac{1}{s}\lim_{N\to\infty}\left\{\sum_{n=1}^{N}\Lambda(n)\,n^{-s}-\Big(\sum_{m\leqslant N}\Lambda(m)\Big)(N+1)^{-s}\right\}=$$

$$=\frac{1}{s}\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}=-\frac{1}{s}\cdot\frac{\zeta'(s)}{\zeta(s)}\quad(\sigma>1).$$

由定理 2.3, 知函數

$$-\frac{1}{s}\frac{\zeta'(s)}{\zeta(s)}-\frac{1}{s-1}=-\frac{1}{s}\left(\frac{\zeta'(s)}{\zeta(s)}+\frac{1}{s-1}\right)-\frac{1}{s}$$

在 $\sigma\geqslant 1$ 時有一級連續導數,故對任意 $a>0$, 在 $1\leqslant\sigma\leqslant 2$, $|t|\leqslant a$ 內一致連續,故有有一級連續導數之函數 $g(t)$, 使

$$\lim_{\sigma\to 1}\left(-\frac{1}{s}\frac{\zeta'(s)}{\zeta(s)}-\frac{1}{s-1}\right)=g(t)$$

在 $|t|\leqslant a$ 中一致成立. 由定理 2 可知

$$\lim_{t\to\infty}e^{-t}\psi(e^t)=1.$$

命 $e^t=x$, 則

$$\lim_{x\to\infty}\frac{\psi(x)}{x}=1.$$

定理得證.

習題 1. 設 p_n 表示第 n 個素數. 試用素數定理證明

$$\lim_{n\to\infty}\frac{p_n}{n\log n}=1.$$

反之,由此也可以推出素數定理.

習題 2. 試由素數定理推出

$$M(x)=\sum_{n\leqslant x}\mu(n)=o(x).$$

習題 3. 試由素數定理推出

$$\sum_{n=1}^{\infty}\frac{\mu(n)}{n}=0.$$

習題 4. 設 $n=p_1^{a_1}\cdots p_k^{a_k}$, 定義

$$\omega(n)=k,\qquad \Omega(n)=a_1+a_2+\cdots+a_k.$$

命

$$\pi_k(x)=\sum_{\substack{n\leqslant x\\ \omega(n)=\Omega(n)=k}}1,\qquad \tau_k(x)=\sum_{\substack{n\leqslant x\\ \Omega(n)=k}}1,$$

$$\vartheta_k(x)=\sum_{p_1\cdots p_k\leqslant x}\log(p_1\cdots p_k),\qquad \prod\nolimits_k(x)=\sum_{p_1\cdots p_k\leqslant x}1.$$

(注意：此處之求和號表示過素數 $p_1,\cdots,p_k$，而具有性質 $p_1\cdots p_k\leqslant x$ 者；同一組 $p_1,\cdots,p_k$ 若次序不同亦算作不同.)

試證：

$$\prod\nolimits_k(x)\sim\frac{kx(\log\log x)^{k-1}}{\log x}\qquad(k\geqslant 2),$$

$$\vartheta_k(x)\sim kx(\log\log x)^{k-1}\qquad(k\geqslant 2),$$

$$\pi_k(x)\sim\tau_k(x)\sim\frac{x(\log\log x)^{k-1}}{(k-1)!\log x}\qquad(k\geqslant 2).$$

§ 6. Selberg 漸近公式.

§6－8 中之 q,r 均表素數，不再一一聲明.

定理 1 (Selberg). 設 $x\geqslant 1$，則

$$\vartheta(x)\log x+\sum_{p\leqslant x}\vartheta\left(\frac{x}{p}\right)\log p=2x\log x+O(x),\tag{1}$$

$$\sum_{p\leqslant x}\log^2 p+\sum_{pq\leqslant x}\log p\log q=2x\log x+O(x).\tag{2}$$

在證明之前先證次引：

引. 若 $F(x),G(x)$ 爲二當 $x\geqslant 1$ 時定義的函數，且

$$G(x)=\sum_{1\leqslant n\leqslant x}F\left(\frac{x}{n}\right)\log x,$$

則

$$\sum_{n\leqslant x}\mu(n)\,G\left(\frac{x}{n}\right)=F(x)\log x+\sum_{n\leqslant x}F\left(\frac{x}{n}\right)\Lambda(n).$$

證： 在 §6.4 中已知 $\Lambda(n)=\sum_{d\mid n}\mu(d)\log\frac{n}{d}$，故

$$\sum_{n\leqslant x}\mu(n)\,G\left(\frac{x}{n}\right)=\sum_{n\leqslant x}\mu(n)\sum_{m\leqslant\frac{x}{n}}F\left(\frac{x}{mn}\right)\log\frac{x}{n}=$$

$$=\sum_{l\leqslant x}F\left(\frac{x}{l}\right)\sum_{n|l}\mu(n)\left(\log\frac{x}{l}+\log\frac{l}{n}\right)=$$

$$=\sum_{l\leqslant x}F\left(\frac{x}{l}\right)\log\frac{x}{l}\cdot\sum_{n|l}\mu(n)+\sum_{l\leqslant x}F\left(\frac{x}{l}\right)\Lambda(l)=$$

$$=F(x)\log x+\sum_{l\leqslant x}F\left(\frac{x}{l}\right)\Lambda(l).$$

定理 1 的證明: 命 γ 表示 Euler 常數,在 §5.8 中已知

$$\sum_{n\leqslant x}\frac{1}{n}=\log x+\gamma+O\left(\frac{1}{x}\right).$$

又

$$\sum_{n\leqslant x}\psi\left(\frac{x}{n}\right)=\sum_{mn\leqslant x}\Lambda(m)=\sum_{n\leqslant x}\sum_{d|n}\Lambda(d)=$$

$$=\sum_{n\leqslant x}\log n=\int_1^x\log t\,dt+O(\log x)=x\log x-x+O(\log x).$$

在引內取

$$F(x)=\psi(x)-x+\gamma+1, \tag{3}$$

故

$$G(x)=\log x\sum_{1\leqslant n\leqslant x}\psi\left(\frac{x}{n}\right)-x\log x\sum_{n\leqslant x}\frac{1}{n}+(\gamma+1)x\log x+O(\log x)=$$

$$=O(\log^2 x)=O(\sqrt{x}).$$

由引卽得

$$F(x)\log x+\sum_{n\leqslant x}F\left(\frac{x}{n}\right)\Lambda(n)=O\left(\sum_{n\leqslant x}\sqrt{\frac{x}{n}}\right)=O(x). \tag{4}$$

由於定理 5.9.1 可知

$$\sum_{n\leqslant x}\frac{\Lambda(n)}{n}=\log x+O(1). \tag{5}$$

故由 (3),(4),(5) 及定理 1.2 可知

$$\psi(x)\log x+\sum_{n\leqslant x}\psi\left(\frac{x}{n}\right)\Lambda(n)=$$

$$=x\log x+x\sum_{n\leqslant x}\frac{\Lambda(n)}{n}-(\gamma+1)\log x-(\gamma+1)\sum_{n\leqslant x}\Lambda(n)+O(x)=$$

$$=2x\log x+O(x). \tag{6}$$

由定理 1.2 可知

$$\sum_{n\leqslant x}\psi\left(\frac{x}{n}\right)\Lambda(n)-\sum_{p\leqslant x}\vartheta\left(\frac{x}{p}\right)\log p=\sum_{mn\leqslant x}\Lambda(m)\Lambda(n)-\sum_{pq\leqslant x}\log p\log q=$$

$$=O\Big(\sum_{\substack{p^\alpha q^\beta\leqslant x\\ \alpha\geqslant 2,\beta\geqslant 1}}\log p\log q\Big)=O\Big(\sum_{\substack{p^\alpha\leqslant x\\ \alpha\geqslant 2}}\log p\sum_{\substack{q^\beta\leqslant x/p^\alpha\\ \beta\geqslant 1}}\log q\Big)=$$

$$=O\Big(\sum_{\substack{p^\alpha\leqslant x\\ \alpha\geqslant 2}}\log p\,\psi\Big(\frac{x}{p^\alpha}\Big)\Big)=O\Big(x\sum_{p\leqslant\sqrt{x}}\sum_{\alpha\geqslant 2}\frac{\log p}{p^\alpha}\Big)$$

$$=O\Big(x\sum_{p\leqslant\sqrt{x}}\frac{\log p}{p(p-1)}\Big)=O(x) \tag{7}$$

及

$$\psi(x)=\vartheta(x)+\vartheta(x^{1/2})+\cdots+\vartheta\Big(x^{\left[\frac{\log 2}{\log x}\right]}\Big)=\vartheta(x)+O(\log x\cdot\vartheta(x^{1/2}))=$$

$$=\vartheta(x)+O(x^{1/2}\log x)\,. \tag{8}$$

由 (6),(7),(8) 卽得 (1) 式.

又由於

$$\vartheta(x)\log x-\sum_{p\leqslant x}\log^2 p=\sum_{p\leqslant x}\log p\log\frac{x}{p}=\sum_{p\leqslant x}\log p\Big(\sum_{n\leqslant\frac{x}{p}}\frac{1}{n}+O(1)\Big)=$$

$$=\sum_{n\leqslant x}\frac{1}{n}\sum_{p\leqslant\frac{x}{n}}\log p+O(\vartheta(x))=$$

$$=O\Big(x\sum_{n\leqslant x}\frac{1}{n^2}\Big)+O(x)=O(x),$$

卽得 (2) 式.

§7. 素數定理的初等證明.

命

$$R(x)=\vartheta(x)-x. \tag{1}$$

由定理 1.1 可知素數定理與

$$\lim_{x\to\infty}\frac{R(x)}{x}=0 \tag{2}$$

等價. 在證明 (2) 式之前,先證以下數引:

引 1. 若 $x\geqslant 3$, 則

$$\sum_{pq\leqslant x}\frac{\log p\log q}{pq}=\frac{1}{2}\log^2 x+O(\log x),$$

$$\sum_{pq\leqslant x}\frac{\log p\log q}{pq\log pq}=\log x+O(\log\log x),$$

$$\sum_{p\leqslant x}\frac{\log p}{p\log\frac{2x}{p}}=O(\log\log x).$$

證：命 $A(n)=\sum_{p\leqslant n}\frac{\log p}{p}$，由定理 5.9.1 可知 $A(n)=\log n+r_n$，而 $r_n=O(1)$. 故

$$\sum_{pq\leqslant x}\frac{\log p\log q}{pq}=\sum_{p\leqslant x}\frac{\log p}{p}\sum_{q\leqslant\frac{x}{p}}\frac{\log q}{q}=\sum_{p\leqslant x}\frac{\log p}{p}\log\frac{x}{p}+O(\log x)=$$

$$=\sum_{n\leqslant x}(A(n)-A(n-1))\log\frac{x}{n}+O(\log x)=$$

$$=\sum_{n\leqslant x-1}A(n)\left\{\log\frac{x}{n}-\log\frac{x}{n+1}\right\}+O(\log x)=$$

$$=\sum_{n\leqslant x}\log n\cdot\log\left(1+\frac{1}{n}\right)+O\left(\sum_{n\leqslant x}\log\left(1+\frac{1}{n}\right)\right)+O(\log x)=$$

$$=\frac{1}{2}\log^2 x+O(\log x).$$

同法，利用上式及分部求和法可知

$$\sum_{pq\leqslant x}\frac{\log p\log q}{pq\log pq}=\log x+O(\log\log x).$$

又由於

$$\sum_{n\leqslant x}\frac{1}{n\log\frac{2x}{n}}=\frac{1}{\log x}\sum_{n\leqslant x}\frac{1}{n}+\sum_{n\leqslant x}\frac{1}{n}\left(\frac{1}{\log\frac{2x}{n}}-\frac{1}{\log x}\right)=$$

$$=\sum_{n\leqslant x}\frac{1}{n}\int_{\frac{2x}{n}}^{x}\frac{du}{u\log^2 u}+O(1)=$$

$$=\int_2^x\frac{\sum_{\frac{2x}{u}\leqslant n\leqslant x}\frac{1}{n}}{u\log^2 u}du+O(1)=\int_2^x\frac{du}{u\log u}+O(1)=O(\log\log x),$$

故

$$\sum_{p\leqslant x}\frac{\log p}{p\log\frac{2x}{p}}=\sum_{n\leqslant x}(A(n)-A(n-1))\frac{1}{\log\frac{2x}{n}}=$$

$$=\sum_{n\leqslant x}\left\{\log n-\log(n-1)\right\}\frac{1}{\log\frac{2x}{n}}+O\left(\sum_{n\leqslant x}r_n\left|\frac{1}{\log\frac{2x}{n}}-\frac{1}{\log\frac{2x}{n+1}}\right|\right)=$$

$$=O\left(\sum_{n\leqslant x}\frac{1}{n\log\frac{2x}{n}}\right)=O(\log\log x).$$

引理證完.

引 2. $\vartheta(x)+\sum_{pq\leqslant x}\frac{\log p\log q}{\log pq}=2x+O\left(\frac{x}{\log x}\right)\quad(x\geqslant 2).$

證: 命 $B(n)=\sum_{pq\leqslant n}\log p\log q,\qquad C(n)=\sum_{p\leqslant n}\log^2 p$, 則

$$\vartheta(x)+\sum_{pq\leqslant x}\frac{\log p\log q}{\log pq}=\sum_{n\leqslant x}\frac{C(n)-C(n-1)}{\log n}+\sum_{n\leqslant x}\frac{B(n)-B(n-1)}{\log n}=$$

$$=\frac{C([x])}{\log[x]}+\frac{B([x])}{\log[x]}+\sum_{n\leqslant x-1}\left\{C(n)+B(n)\right\}\left\{\frac{1}{\log n}-\frac{1}{\log(n+1)}\right\}=$$

$$=2x+O\left(\frac{x}{\log x}\right)+\sum_{n\leqslant x-1}\left(2n\log n+O(n)\right)\frac{\log\left(1+\frac{1}{n}\right)}{\log n\log(n+1)}=$$

$$=2x+O\left(\frac{x}{\log x}\right).$$

引理證畢.

引 3. $R(x)\log x=\sum_{pq\leqslant x}\frac{\log p\log q}{\log pq}R\left(\frac{x}{pq}\right)+O(x\log\log x)\quad(x\geqslant 3).$

證: 由引 1 及引 2 得

$$\sum_{p\leqslant x}\vartheta\left(\frac{x}{p}\right)\log p=2x\sum_{p\leqslant x}\frac{\log p}{p}-\sum_{p\leqslant x}\log p\sum_{qr\leqslant\frac{x}{p}}\frac{\log q\log r}{\log qr}+$$

$$+O\left(x\sum_{p\leqslant x}\frac{\log p}{p\log\frac{2x}{p}}\right)=$$

$$= 2x\log x - \sum_{qr\leqslant x}\frac{\log q\log r}{\log qr}\vartheta\left(\frac{x}{qr}\right) + O(x\log\log x).$$

將此式代入 Selberg 公式（卽（6.1）式），得

$$\vartheta(x)\log x = \sum_{pq\leqslant x}\frac{\log p\log q}{\log pq}\vartheta\left(\frac{x}{pq}\right) + O(x\log\log x).$$

將（1）式代入上式，由引 1 卽得本引理。

引 4. $|R(x)| \leqslant \frac{1}{\log x}\sum_{n\leqslant x}\left|R\left(\frac{x}{n}\right)\right| + O\left(\frac{x\log\log x}{\log x}\right) \quad (x\geqslant 3).$

證：將 (1) 式代入 (6.1) 式得

$$R(x)\log x = -\sum_{p\leqslant x}R\left(\frac{x}{p}\right)\log p + O(x),$$

故由引 3 可知

$$2|R(x)|\log x \leqslant \sum_{p\leqslant x}\left|R\left(\frac{x}{p}\right)\right|\log p + \sum_{pq\leqslant x}\frac{\log p\log q}{\log pq}\left|R\left(\frac{x}{pq}\right)\right| + O(x\log\log x).$$

由引 2 及分部求和法，並注意 $\big||a|-|b|\big|\leqslant|a-b|$，故

$$2|R(x)|\log x \leqslant \sum_{n\leqslant x-1}\left(\sum_{p\leqslant n}\log p + \sum_{pq\leqslant n}\frac{\log p\log q}{\log pq}\right)\left(\left|R\left(\frac{x}{n}\right)\right| - \left|R\left(\frac{x}{n+1}\right)\right|\right) +$$
$$+ O\left(\sum_{p\leqslant x}\log p + \sum_{pq\leqslant x}\frac{\log p\log q}{\log pq}\right) + O(x\log\log x) \leqslant$$
$$\leqslant 2\sum_{n\leqslant x-1}n\left(\left|R\left(\frac{x}{n}\right)\right| - \left|R\left(\frac{x}{n+1}\right)\right|\right) +$$
$$+ O\left(\sum_{n\leqslant x-1}\frac{n}{\log 2n}\left|\left|R\left(\frac{x}{n}\right)\right| - \left|R\left(\frac{x}{n+1}\right)\right|\right|\right) +$$
$$+ O(x\log\log x) \leqslant$$
$$\leqslant 2\sum_{n\leqslant x}\left|R\left(\frac{x}{n}\right)\right| + O\left(\sum_{n\leqslant x-1}\frac{n}{\log 2n}\left(\vartheta\left(\frac{x}{n}\right) - \vartheta\left(\frac{x}{n+1}\right)\right)\right) +$$
$$+ O\left(x\sum_{n\leqslant x-1}\frac{n}{\log 2n}\left(\frac{1}{n} - \frac{1}{n+1}\right)\right) + O(x\log\log x).$$

由定理 1.2 可知

$$\sum_{n\leqslant x-1}\frac{n}{\log 2n}\left(\vartheta\left(\frac{x}{n}\right)-\vartheta\left(\frac{x}{n+1}\right)\right)=$$

$$=\sum_{2\leqslant n\leqslant x-1}\vartheta\left(\frac{x}{n}\right)\left(\frac{n}{\log 2n}-\frac{n-1}{\log 2(n-1)}\right)+O(x)=$$

$$=O\left(x\sum_{n\leqslant x}\frac{1}{n\log n}\right)=O(x\log\log x),$$

故

$$2\mid R(x)\mid\log x\leqslant 2\sum_{n\leqslant x}\left|R\left(\frac{x}{n}\right)\right|+O(x\log\log x).$$

明所欲證.

引 5. 若 $x>1$, 則

$$\sum_{n\leqslant x}\frac{\vartheta(n)}{n^2}=\log x+O(1),$$

$$\sum_{n\leqslant x}\vartheta\left(\frac{x}{n}\right)=x\log x+O(x).$$

證: 因

$$\sum_{p\leqslant n\leqslant x}\frac{1}{n^2}=\sum_{n\geqslant p}\frac{1}{n^2}-\sum_{n>x}\frac{1}{n^2}=\frac{1}{p}+O\left(\frac{1}{p^2}\right)+O\left(\frac{1}{x}\right),$$

故

$$\sum_{n\leqslant x}\frac{\vartheta(n)}{n^2}=\sum_{n\leqslant x}\frac{1}{n^2}\sum_{p\leqslant n}\log p=\sum_{p\leqslant x}\log p\sum_{p\leqslant n\leqslant x}\frac{1}{n^2}=$$

$$=\sum_{p\leqslant x}\log p\left(\frac{1}{p}+O\left(\frac{1}{p^2}\right)+O\left(\frac{1}{x}\right)\right)=\log x+O(1).$$

又

$$\sum_{n\leqslant x}\vartheta\left(\frac{x}{n}\right)=\sum_{n\leqslant x}\sum_{p\leqslant\frac{x}{n}}\log p=\sum_{p\leqslant x}\log p\sum_{n\leqslant\frac{x}{p}}1=$$

$$=\sum_{p\leqslant x}\log p\cdot\left(\frac{x}{p}+O(1)\right)=x\log x+O(x).$$

引 6. $\displaystyle\sum_{n\leqslant x}\frac{\log n}{n}R(n)=-\sum_{n\leqslant x}\frac{1}{n}R(n)R\left(\frac{x}{n}\right)+O(x).$

證: 由 Selberg 公式 (卽 (6.2) 式) 及分部求和法可知

$$\sum_{p\leqslant x}\log^2 p\log\frac{x}{p}+\sum_{pq\leqslant x}\log p\log q\log\frac{x}{pq}=2x\log x+O(x).$$

由於

$$\log\frac{x}{p}=\sum_{p\leqslant n\leqslant x}\frac{1}{n}+O\left(\frac{1}{p}\right),\qquad \log\frac{x}{pq}=\sum_{p\leqslant n\leqslant\frac{x}{q}}\frac{1}{n}+O\left(\frac{1}{p}\right),$$

代入上式並交換和號,可知

$$\sum_{n\leqslant x}\frac{1}{n}\sum_{p\leqslant n}\log^2 p+\sum_{n\leqslant x}\frac{1}{n}\sum_{p\leqslant n}\log p\sum_{q\leqslant\frac{x}{n}}\log q=2x\log x+O(x),$$

卽得

$$\sum_{n\leqslant x}\frac{\log n}{n}\vartheta(n)+\sum_{n\leqslant x}\frac{1}{n}\vartheta(n)\,\vartheta\left(\frac{x}{n}\right)=2x\log x+O(x).$$

將 (1) 式代入上式,並利用引 5, 卽得引理.

引 7. 若 $0<\sigma<1$, 且存在 x_0, 當 $x>x_0$ 時有

$$|R(x)|<\sigma x, \tag{3}$$

則存在 x_σ, 當 $x>x_\sigma$ 時, 區間 $((1-\sigma)^{16}x, x)$ 皆包含一個子區間 $(y, e^\delta y)$, 當 $y\leqslant z\leqslant e^\delta y$ 時

$$\left|\frac{R(z)}{z}\right|<\frac{\sigma+\sigma^2}{2},$$

此處 $\delta=\dfrac{\sigma(1-\sigma)}{32}$.

證: 由引 6 可知

$$\left|\sum_{n<x}\frac{\log n}{n}R(n)\right|\leqslant\left|\sum_{x_0\leqslant n\leqslant\frac{x}{x_0}}\frac{1}{n}R(n)\,R\left(\frac{x}{n}\right)\right|+$$

$$+\left|\sum_{n<x_0}\frac{1}{n}R(n)\,R\left(\frac{x}{n}\right)\right|+\left|\sum_{\frac{x}{x_0}<n\leqslant x}\frac{1}{n}R(n)\,R\left(\frac{x}{n}\right)\right|+O(x)\leqslant$$

$$\leqslant\sigma^2 x\sum_{x_0\leqslant n\leqslant\frac{x}{x_0}}\frac{1}{n}+O(x)=\sigma^2 x\log x+O(x),$$

故當 $x>x_1$ 時,

$$\left|\sum_{x'\leqslant n\leqslant x}\frac{\log n}{n}R(n)\right|<\sigma^2(x+x')\log x+O(x),$$

此處 $x'=(1-\sigma)^{16}x$.

倘若 $R(n)$ 在 (x',x) 內不變號,則必有 y $(x'\leqslant y\leqslant x)$, 使

$$\left|\frac{R(y)}{y}\right|\sum_{x'\leqslant n\leqslant x}\log n<\sigma^2(x+x')\log x+O(x).$$

由於 $(1-\sigma)^{16}<\dfrac{1-\sigma}{1+15\sigma}$,故

$$\left|\frac{R(y)}{y}\right|<\sigma^2\frac{x+x'}{x-x'}+O\left(\frac{1}{\log x}\right)<\frac{\sigma(1+7\sigma)}{8}+O\left(\frac{1}{\log x}\right)<$$

$$<\frac{\sigma(1+3\sigma)}{4}\quad(x>x_1).\tag{4}$$

但若 $R(n)$ 在 (x',x) 內變號,則顯然有 y $(x'\leqslant y\leqslant x)$ 使 $|R(y)|=O(\log y)$, 故 (4) 式仍成立.

當 $1<y<y'$ 時,由引 2 可知

$$\sum_{y<p\leqslant y'}\log p\leqslant 2(y'-y)+O\left(\frac{y'}{\log y'}\right).$$

由 (1) 式卽得

$$|R(y')-R(y)|<(y'-y)+O\left(\frac{y'}{\log y'}\right).\tag{5}$$

命 $x'\leqslant y_1,y_2\leqslant x$, y_1 適合 (4) 式及 $e^{-\delta}\leqslant\dfrac{y_2}{y_1}\leqslant e^{\delta}$. 由 (4), (5) 可知

$$\left|\frac{R(y_2)}{y_2}\right|<\left|\frac{R(y_1)}{y_1}\right|\cdot\frac{y_1}{y_2}+\left|1-\frac{y_1}{y_2}\right|+O\left(\frac{1}{\log x}\right)<$$

$$<\frac{\sigma(1+3\sigma)}{4}\cdot e^{\delta}+(e^{\delta}-1)+O\left(\frac{1}{\log x}\right).$$

由於 $e^{\delta}<\dfrac{1}{1-\delta}$ $(0<\delta<1)$, 故

$$\left|\frac{R(y_2)}{y_2}\right|<\frac{\sigma(1+3\sigma)}{4}\cdot\frac{1}{1-\delta}+\left(\frac{1}{1-\delta}-1\right)+O\left(\frac{1}{\log x}\right)<$$

$$<\frac{\sigma(3+5\sigma)}{8}+O\left(\frac{1}{\log x}\right)<\frac{\sigma+\sigma^2}{4}\quad(x>x_0).$$

當 $y_1 \leqslant \frac{1+7\sigma}{1+15\sigma}x$ 時，可知 $e^{\delta}y_1 < x$，故取 $y = y_1$ 卽合所需. 當 $y_1 > \frac{1+7\sigma}{1+15\sigma}x$ 時，則 $e^{-\delta}y_1 > \frac{1-\sigma}{1+15\sigma}x > x_1$，故取 $y = e^{-\delta}y_1$ 卽合所需.

引理證畢.

素數定理的證明： 已知存在 $c > 0$ 及 x_0'，當 $x > x_0'$ 時有

$$\vartheta(x) > cx \tag{6}$$

(此卽定理 1.2). 由 Selberg 公式可得

$$\vartheta(x) = 2x - \frac{1}{\log x}\sum_{p\leqslant x}\vartheta\left(\frac{x}{p}\right)\log p + O\left(\frac{x}{\log x}\right) =$$

$$= 2x - \frac{1}{\log x}\sum_{p<\frac{x}{x_0'}}\vartheta\left(\frac{x}{p}\right)\log p - \frac{1}{\log x}\sum_{\frac{x}{x_0'}<p\leqslant x}\vartheta\left(\frac{x}{p}\right)\log p + O\left(\frac{x}{\log x}\right) \leqslant$$

$$\leqslant 2x - \frac{cx\log x}{\log x} + O\left(\frac{1}{\log x}\sum_{\frac{x}{x_0'}<p\leqslant x}\log p\right) + O\left(\frac{x}{\log x}\right) =$$

$$= (2-c)x + O\left(\frac{x}{\log x}\right) < \left(2-\frac{c}{2}\right)x \quad (x > x_0,\ c > 0).$$

由 (1) 式卽得

$$|R(x)| < \sigma_0 x \quad \left(x > x_0,\quad \sigma_0 = \left|1-\frac{c}{2}\right|,\quad 0 < \sigma_0 < 1\right).$$

命

$$\zeta = (1-\sigma_0)^{-16},\quad \delta = \frac{\sigma_0(1-\sigma_0)}{32}.$$

由引 7 得知存在 $x_{\sigma_0} > x_0$，當 $x > x_{\sigma_0}$ 時，任何區間 $(\zeta^{\nu-1}, \zeta^{\nu})\left(\zeta \leqslant \zeta^{\nu} \leqslant \frac{x}{x_{\sigma_0}}\right)$ 都包有子區間 $(y_\nu, e^{\delta}y_\nu)$，當 $y_\nu \leqslant n \leqslant e^{\delta}y_\nu$ 時，

$$\left|\frac{n}{x}R\left(\frac{x}{n}\right)\right| < \frac{\sigma_0+\sigma_0^2}{2}.$$

由引 4 可知

$$|R(x)| < \frac{1}{\log x}\sum_{n\leqslant\frac{x}{x_{\sigma_0}}}\left|R\left(\frac{x}{n}\right)\right| + \frac{1}{\log x}\sum_{\frac{x}{x_{\sigma_0}}<n\leqslant x}\left|R\left(\frac{x}{n}\right)\right| + O\left(\frac{x}{\sqrt{\log x}}\right) <$$

$$< \frac{\sigma_0 x}{\log x}\sum_{\substack{1\leqslant n\leqslant\frac{x}{x_{\sigma_0}}\\ n\notin(y_\nu, e^{\delta}y_\nu)}}\frac{1}{n} + \frac{\sigma_0+\sigma_0^2}{2}\cdot\frac{x}{\log x}\sum_{\zeta^{\nu}\leqslant\frac{x}{x_{\sigma_0}}}\ \sum_{y_\nu\leqslant n\leqslant e^{\delta}y_\nu}\frac{1}{n} + O\left(\frac{x}{\sqrt{\log x}}\right) <$$

$$< \frac{\sigma_0 x}{\log x} \sum_{n \leqslant \frac{x}{x_{\sigma_0}}} \frac{1}{n} - \frac{(\sigma_0 - \sigma_0^2)}{2} \cdot \frac{x}{\log x} \sum_{\zeta^\nu \leqslant \frac{x}{x_{\sigma_0}}} \sum_{y_\nu \leqslant n \leqslant e^\delta y_\nu} \frac{1}{n} + O\left(\frac{x}{\sqrt{\log x}}\right) <$$

$$< \sigma_0 x - \frac{(\sigma_0 - \sigma_0^2)}{2} \cdot \frac{x}{\log x} \sum_{\zeta^\nu \leqslant \frac{x}{x_{\sigma_0}}} \left(\delta + O\left(\frac{1}{\zeta^\nu}\right)\right) + O\left(\frac{x}{\sqrt{\log x}}\right) <$$

$$< \sigma_0 x - \frac{(\sigma_0 - \sigma_0^2)}{2} \cdot \frac{x}{\log x} \cdot \frac{\delta \log x}{\log \zeta} + O\left(\frac{x}{\sqrt{\log x}}\right) <$$

$$< \sigma_0 \left(1 - \frac{(1-\sigma_0)^2 \sigma_0}{1024 \log \frac{1}{1-\sigma_0}}\right) x + O\left(\frac{x}{\sqrt{\log x}}\right) <$$

$$< \sigma_0 \left(1 - \frac{(1-\sigma_0)^3}{1024}\right) x + O\left(\frac{x}{\sqrt{\log x}}\right) <$$

$$< \sigma_0 \left(1 - \frac{(1-\sigma_0)^3}{2000}\right) x = \sigma_1 x \quad (x > x_{\sigma_1} > x_{\sigma_0}),$$

此處 $\sigma_1 < \sigma_0$. 不斷用上面的手續得到

$$|R(x)| < \sigma_n x \qquad (x > x_{\sigma_n}),$$

此處 $\sigma_n = \sigma_{n-1}\left(1 - \frac{(1-\sigma_{n-1})^3}{2000}\right) \leqslant \sigma_{n-1}\left(1 - \frac{(1-\sigma_0)^3}{2000}\right) \leqslant \cdots \leqslant$

$$\leqslant \sigma_0 \left(1 - \frac{(1-\sigma_0)^3}{2000}\right)^n, \quad 故 \quad \lim_{n \to \infty} \sigma_n = 0.$$

明所欲證.

§ 8. Dirichlet 定理:

定理 1 (Dirichlet). 若 $k > 0$, $l > 0$, $(k, l) = 1$, 則形如 $kn + l$ 之素數之個數無窮.

本節將證明下面較定理 1 強的定理:

定理 2. 若 $k > 0$, $l > 0$, $(k, l) = 1$, 則

$$\sum_{\substack{p \leqslant x \\ p \equiv l \pmod{k}}} \frac{\log p}{p} = \frac{1}{\varphi(k)} \log x + O(1),$$

此處 $\sum_{\substack{p \leqslant x \\ p \equiv l \pmod{k}}}$ 表示就所有不超過 x 的形如 $kn + l$ 的素數求和. 與 O 有關之常數僅與 k 有關.

證明定理 2 之前需要下面數引:

若 χ 爲非主特徵,命

$$L(\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n},\qquad L_1(\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)\log n}{n}. \tag{1}$$

引 1. 設 χ 是非主特徵之實特徵,則 $L(\chi)\neq 0$.

證: 命

$$F(n)=\sum_{d|n}\chi(d).$$

由於

$$F(p^l)=\begin{cases}1+1+\cdots+1=l+1, & 若\ \chi(p)=1,\\ 1-1+\cdots+1=1, & 若\ \chi(p)=-1,\ l\ 爲偶數,\\ 1-1+\cdots-1=0, & 若\ \chi(p)=-1,\ l\ 爲奇數,\end{cases}$$

而 $F(n)$ 又是積性函數,故

$$F(n)\geqslant\begin{cases}1, & 若\ n\ 爲完全平方,\\ 0, & 其他情形,\end{cases}$$

故

$$G(x)=\sum_{n\leqslant x}\frac{F(n)}{n^{1/2}}\geqslant\sum_{1\leqslant m\leqslant\sqrt{x}}\frac{1}{m}\to\infty.$$

但另一方面,由於當 χ 非主特徵時,有

$$\sum_{x<n\leqslant y}\frac{\chi(n)}{n^{\delta}}=O(x^{-\delta}),\quad\sum_{x<n\leqslant y}\frac{\chi(n)\log n}{n^{\delta}}=O\left(\frac{\log x}{x^{\delta}}\right)\quad(\delta>0,x>1). \tag{2}$$

(此可由習題 7.2.1 及定理 6.8.2 得之.)故由例 5.8.4 得.

$$G(x)=\sum_{n\leqslant x}\frac{1}{n^{1/2}}\sum_{d|n}\chi(d)=\sum_{dd'\leqslant x}\frac{\chi(d)}{d^{1/2}d'^{1/2}}=$$

$$=\sum_{d'\leqslant\sqrt{x}}\frac{1}{d'^{1/2}}\sum_{\sqrt{x}<d\leqslant\frac{x}{d'}}\frac{\chi(d)}{d^{1/2}}+\sum_{d\leqslant\sqrt{x}}\frac{\chi(d)}{d^{1/2}}\sum_{d'\leqslant\frac{x}{d}}\frac{1}{d'^{1/2}}=$$

$$=\sum_{d'\leqslant\sqrt{x}}\frac{1}{d'^{1/2}}\left\{O(x^{-\frac{1}{4}})\right\}+\sum_{d\leqslant\sqrt{x}}\frac{\chi(d)}{d^{1/2}}\left\{2\sqrt{\frac{x}{d}}+c_1+O\left(\sqrt{\frac{d}{x}}\right)\right\}=$$

$$= 2\sqrt{x} \sum_{d \leqslant \sqrt{x}} \frac{\chi(d)}{d} + O(1) =$$

$$= 2\sqrt{x}\, L(\chi) + O(1)\,.$$

若 $L(\chi) = 0$, 則 $G(x) = O(1)$. 此不可能,故得引理.

引 2. $L_1(\chi) \sum_{n \leqslant x} \frac{\mu(n)\chi(n)}{n} = \begin{cases} O(1), & \text{若} \quad L(\chi) \neq 0, \\ -\log x + O(1), & \text{若} \quad L(\chi) = 0. \end{cases}$

證: 在定理 6.3.3 內命 $H(n) = \chi(n)$, $F(n) = n$, 則由

$$G(x) = \sum_{1 \leqslant n \leqslant x} F\left(\frac{x}{n}\right) H(n) = x \sum_{1 \leqslant n \leqslant x} \frac{\chi(n)}{n} = x\, L(\chi) + O(1),$$

故

$$x = F(x) = \sum_{1 \leqslant n \leqslant x} \mu(n)\, G\left(\frac{x}{n}\right) H(n) = x\, L(\chi) \sum_{1 \leqslant n \leqslant x} \frac{\chi(n)\mu(n)}{n} + O(x),$$

卽得

$$L(\chi) \sum_{n \leqslant x} \frac{\mu(n)\chi(n)}{n} = O(1)\,.$$

若 $L(\chi) \neq 0$, 則 $\sum_{n \leqslant x} \frac{\mu(n)\chi(n)}{n} = O(1)$, 卽得定理. 但若 $L(\chi) = 0$, 則在定理 6.3.3 內命 $F(x) = x \log x$, $H(n) = \chi(n)$,故

$$G(x) = \sum_{n \leqslant x} F\left(\frac{x}{n}\right) H(n) = x \sum_{n \leqslant x} \frac{\chi(n)}{n} \log \frac{x}{n} = .$$

$$= L(\chi)\, x \log x - L_1(\chi)\, x + O(\log x) =$$

$$= -L_1(\chi)\, x + O(\log x).$$

由於例 5.8.2 可知 $\sum_{n \leqslant x} \log \frac{x}{n} = O(x)$,故

$$x \log x = \sum_{1 \leqslant n \leqslant x} \mu(n)\, G\left(\frac{x}{n}\right) H(n) = \sum_{n \leqslant x} \mu(n)\chi(n) \left\{ -L_1(\chi) \frac{x}{n} + \right.$$

$$\left. + O\left(\log \frac{x}{n}\right) \right\} = -L_1(\chi)\, x \sum_{n \leqslant x} \frac{\mu(n)\chi(n)}{n} + O(x).$$

引理證畢.

引 3. $\sum_{p\leqslant x}\frac{\chi(p)\log p}{p}=\begin{cases}O(1), & 若\ L(\chi)\neq 0,\\ -\log x+O(1), & 若\ L(\chi)=0.\end{cases}$

證: $$\sum_{p\leqslant x}\frac{\chi(p)\log p}{p}=\sum_{n\leqslant x}\frac{\chi(n)\Lambda(n)}{n}+O(1)=$$

$$=\sum_{n\leqslant x}\frac{\chi(n)}{n}\sum_{d|n}\mu(d)\log\frac{n}{d}+O(1)=$$

$$=\sum_{dd'\leqslant x}\frac{\chi(d)\chi(d')}{dd'}\mu(d)\log d'+O(1)=$$

$$=\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d}\sum_{d'\leqslant\frac{x}{d}}\frac{\chi(d')\log d'}{d'}+O(1)=$$

$$=\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d}\left\{L_1(\chi)+O\left(\frac{\log\frac{x}{d}}{x/d}\right)\right\}+O(1)=$$

$$=L_1(\chi)\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d}+O(1).$$

故由引 2 卽得所欲.

引 4. 設 χ 爲非主特徵，則 $L(\chi)\neq 0$.

證: 設 N 爲 mod k 之非主特徵之中，使 $L(\chi)=0$ 者之個數. 又以 $\sum_{(\chi)}$ 表示過 mod k 所有的特徵. 則由引 3 及定理 7.2.4 與定理 7.2.5 得

$$\varphi(k)\sum_{\substack{p\leqslant x\\ p\equiv 1(\text{mod}\,k)}}\frac{\log p}{p}=\sum_{(\chi)}\sum_{p\leqslant x}\frac{\chi(p)\log p}{p}=\sum_{\substack{p\leqslant x\\ p\nmid k}}\frac{\log p}{p}+\sum_{\substack{\chi\neq\chi_0\\(\chi)}}\sum_{p\leqslant x}\frac{\chi(p)\log p}{p}=$$
$$=(1-N)\log x+O(1).$$

但因 $\varphi(k)\sum_{\substack{p\leqslant x\\ p\equiv 1(\text{mod}\,k)}}\frac{\log p}{p}\geqslant 0$, 故必 $0\leqslant N\leqslant 1$. 又倘若 χ 是複特徵，則必 $L(\chi)\neq 0$; 否則亦得 $L(\bar{\chi})=0$, 則 $N\geqslant 2$ 矣. 而當 χ 是實特徵時，由引 1 知 $L(\chi)\neq 0$, 故 $N=0$. 引理得證.

定理 2 的證明: 由引 3 及引 4 得

$$\sum_{p\leqslant x}\frac{\chi(p)\log p}{p}=O(1),$$

故由習題 7.2.2 得

$$\varphi(k)\sum_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\frac{\log p}{p}=\sum_{(\chi)}\bar{\chi}(l)\sum_{p\leqslant x}\frac{\chi(p)\log p}{p}=$$

$$=\sum_{\substack{p\leqslant x\\ p\nmid k}}\frac{\log p}{p}+\sum_{\substack{(\chi)\\ \chi\neq\chi_0}}\bar{\chi}(l)\sum_{p\leqslant x}\frac{\chi(p)\log p}{p}=\log x+O(1).$$

明所欲證。

習題. 若 $(k,l)=1,\ l\leqslant k$. 試證

$$\lim_{x\to\infty}\frac{\pi(x;k,l)}{\dfrac{x}{\varphi(k)\log x}}=1.$$

提示: 1) 命

$$\vartheta_l(x)=\sum_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\log p,\qquad \psi_l(x)=\sum_{\substack{n\leqslant x\\ n\equiv l(\bmod k)}}\Lambda(n),$$

則

$$\varlimsup_{x\to\infty}\frac{\pi(x;k,l)}{\dfrac{x}{\varphi(k)\log x}}=\varlimsup_{x\to\infty}\frac{\vartheta_l(x)}{\dfrac{x}{\varphi(k)}}=\varlimsup_{x\to\infty}\frac{\psi_l(x)}{\dfrac{x}{\varphi(k)}};$$

$$\varliminf_{x\to\infty}\frac{\pi(x;k,l)}{\dfrac{x}{\varphi(k)\log x}}=\varliminf_{x\to\infty}\frac{\vartheta_l(x)}{\dfrac{x}{\varphi(k)}}=\varliminf_{x\to\infty}\frac{\psi_l(x)}{\dfrac{x}{\varphi(k)}}.$$

2) 證明: $\displaystyle\sum_{d|n}\mu(d)\log^2\frac{n}{d}=\Lambda(n)\log n+\sum_{d|n}\Lambda(d)\Lambda\left(\frac{n}{d}\right).$

將上式兩邊關於 n 求和,求和的範圍為: $1\leqslant n\leqslant x,\ n\equiv l\ (\bmod k)$, 則得

$$\sum_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\log^2 p+\sum_{\substack{pq\leqslant x\\ pq\equiv l(\bmod k)}}\log p\log q=\frac{2}{\varphi(k)}x\log x+O(x)$$

及

$$\vartheta_l(x)\log x+\sum_{p\leqslant x}\log p\,\vartheta_{l\bar{p}}\left(\frac{x}{p}\right)=\frac{2}{\varphi(k)}x\log x+O(x),$$

此處 $\bar{p}$ 為同餘式 $p\bar{p}\equiv1\ (\bmod k)$ 的解。

3) 命

$$\vartheta_l(x)=\frac{x}{\varphi(k)}+R_l(x),$$

則

$$R_l(x)\log x=\sum_{pq\leqslant x}\frac{\log p\log q}{\log pq}R_{l\overline{pq}}\left(\frac{x}{pq}\right)+O(x\log\log x).$$

4) $$|R_l(x)|\leqslant\frac{1}{\varphi(k)\log x}\sum_{\substack{1\leqslant a\leqslant k\\(a,k)=1}}\sum_{n\leqslant x}\left|R_a\left(\frac{x}{n}\right)\right|+O\left(\frac{x\log\log x}{\log x}\right).$$

5) $$\sum_{n\leqslant x}\frac{\log n}{n}R_l(n)=-\sum_{n\leqslant x}\frac{1}{n}\sum_{a\beta\equiv l(\bmod k)}R_a(n)R_\beta\left(\frac{x}{n}\right)+O(x).$$

6) 若 $0<\sigma<1$，且存在 x_0，當 $x>x_0$ 時，$|R_l(x)|<\frac{\sigma x}{\varphi(k)}$，則必存在 x_σ，當 $x>x_\sigma$ 時，區間 $((1-\sigma)^{16}x,x)$ 皆包含一個子區間 $(y,e^\delta y)$ $\left(\delta=\frac{\sigma(1-\sigma)}{32}\right)$，當 $y\leqslant z\leqslant e^\delta y$ 時，

$$\left|\frac{R_l(z)}{z}\right|<\frac{1}{\varphi(k)}\cdot\frac{\sigma+\sigma^2}{2}.$$

7) 試先由定理 2 導出存在 σ_0 及 x_0，而 $0<\sigma_0<1$，當 $x>x_0$ 時，

$$|R_l(x)|<\frac{\sigma_0}{\varphi(k)}x.$$

再由此並利用 4),6) 卽可證明

$$\lim_{x\to\infty}\frac{R_l(x)}{x}=0.$$

第　十　章

漸近法與連分數

§ 1. 簡單連分數. 分數

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{\ddots}{\quad + \cfrac{1}{a_N}}}}}$$

謂之有限連分數 (finite continued fraction). 若 $N=\infty$, 則簡稱連分數, 此時之連分數之確實代表一數, 將於以後證明. 上之寫法頗佔篇幅. 故通常以符號:

$$a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_N}$$

或

$$[a_0, a_1, a_2, \cdots, a_N]$$

來表示. 由計算易得

$$[a_0] = \frac{a_0}{1}, \quad [a_0, a_1] = \frac{a_0 a_1 + 1}{a_1}, \quad [a_0, a_1, a_2] = \frac{a_2 a_1 a_0 + a_2 + a_0}{a_2 a_1 + 1}.$$

普通寫

$$[a_0, a_1, \cdots, a_n] = \frac{p_n}{q_n}, \qquad 0 \leqslant n \leqslant N,$$

其中 p_n 及 q_n 爲 $a_0, a_1, \cdots, a_n$ 之多項式. 對任一 a 皆爲一次式. 其分母 q_n 與 a_0 無關. $\frac{p_n}{q_n}$ 名爲 $[a_0, \cdots, a_N]$ 之第 n 個漸近值或漸近分數 (n-th convergent).

定 理 1. 諸漸近值間有次之關係:

$$p_0 = a_0, \quad p_1 = a_1 a_0 + 1, \quad p_n = a_n p_{n-1} + p_{n-2} \qquad (2 \leqslant n \leqslant N),$$

$$q_0 = 1, \quad q_1 = a_1, \qquad q_n = a_n q_{n-1} + q_{n-2} \qquad (2 \leqslant n \leqslant N).$$

證: $n = 0, 1$ 及 2 時,可以直接從運算得之,設 $m < N$, 且假定

$$[a_0, \cdots, a_m] = \frac{p_m}{q_m} = \frac{a_m p_{m-1} + p_{m-2}}{a_m q_{m-1} + q_{m-2}},$$

此處 $p_{m-1}, q_{m-1}, p_{m-2}, q_{m-2}$ 皆祇與 $a_0, \cdots, a_{m-1}$ 有關. 進而用歸納法以證明定理. 因

$$\frac{p_{m+1}}{q_{m+1}} = [a_0, \cdots, a_m, a_{m+1}] = \left[a_0, \cdots, a_{m-1}, a_m + \frac{1}{a_{m+1}}\right] =$$

$$= \frac{\left(a_m + \frac{1}{a_{m+1}}\right) p_{m-1} + p_{m-2}}{\left(a_m + \frac{1}{a_{m+1}}\right) q_{m-1} + q_{m-2}} = \frac{a_{m+1}(a_m p_{m-1} + p_{m-2}) + p_{m-1}}{a_{m+1}(a_m q_{m-1} + q_{m-2}) + q_{m-1}} =$$

$$= \frac{a_{m+1} p_m + p_{m-1}}{a_{m+1} q_m + q_{m-1}}.$$

故得定理.

定理 2. p_n 及 q_n 適合下列諸式:

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1} \qquad (n \geqslant 1), \tag{1}$$

即

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}}$$

及

$$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n \qquad (n \geqslant 2). \tag{2}$$

證: (1) 對 $n = 1$ 時顯然成立. 用歸納法及定理 1,

$$p_n q_{n-1} - p_{n-1} q_n = (a_n p_{n-1} + p_{n-2}) q_{n-1} - p_{n-1}(a_n q_{n-1} + q_{n-2}) = (-1)^{n-1}.$$

又由定理 1 及 (1) 式可得

$$p_n q_{n-2} - p_{n-2} q_n = (a_n p_{n-1} + p_{n-2}) q_{n-2} - p_{n-2}(a_n q_{n-1} + q_{n-2}) =$$
$$= a_n (p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) = (-1)^n a_n.$$

定義. 若 a_0 爲整數, $a_1, a_2, \cdots$ 皆爲正整數. 則

$$a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots$$

謂之簡單連分數,本章所論僅限於簡單連分數.

由定理 1 及 2 可立得次之諸簡單結論:

定理 3. (i) 當 $n>1$, 則 $q_n \geqslant q_{n-1}+1$, 故 $q_n \geqslant n$.

(ii) $\frac{p_{2n+1}}{q_{2n+1}} < \frac{p_{2n-1}}{q_{2n-1}}$, $\frac{p_{2n}}{q_{2n}} > \frac{p_{2n-2}}{q_{2n-2}}$.

(iii) 凡簡單連分數之漸近分數,皆爲既約分數.

命 α 爲一實數. 取 $a_0=[\alpha]$,命

$$\alpha_1'=\frac{1}{\alpha-[\alpha]}, \quad 取 \quad a_1=[\alpha_1'].$$

再命

$$\alpha_2'=\frac{1}{\alpha_1'-[\alpha_1']}, \quad 取 \quad a_2=[\alpha_2'].$$

續行此法. 命

$$\frac{1}{\alpha_{n-1}'-[\alpha_{n-1}']}=\alpha_n', \quad 取 \quad a_n=[\alpha_n']$$

等等. 顯然, 若祇能做有限步, 則 α 必爲有理數. 反之, 若 α 爲有理數 $\frac{p}{q}$, $(p, q)=1$, 則 $a_0=\left[\frac{p}{q}\right]$,而

$$\frac{1}{\alpha_1'}=\frac{p}{q}-\left[\frac{p}{q}\right], \qquad 0 \leqslant \frac{1}{\alpha_1'}<1,$$

即

$$p-\left[\frac{p}{q}\right]q=\frac{q}{\alpha_1'}(=r_1), \qquad 0 \leqslant r_1<q.$$

又同法

$$q-r_1\left[\frac{q}{r_1}\right]=\frac{r_1}{\alpha_2'}(=r_2), \qquad 0 \leqslant r_2<r_1.$$

故若 α 爲有理數,則連分數之計算與 Euclid 計算法 (輾轉相除法) 有貌異實同之妙. 且屢次所得之商即爲 $a_0, a_1, a_2, \cdots$, 故得次之定理:

定理 4. 凡有理數必可表爲有限連分數.

刻下立即發生次之問題,即表法爲唯一否? 由顯然例證:

$$a+\frac{1}{1}=a+1$$

可見表法非一. 換言之, 若 $a_n>1$, 則

$$[a_0, \cdots, a_n] = [a_0, \cdots, a_{n-1}, a_n - 1, 1];$$

若 $a_n = 1$，則有

$$[a_0, \cdots, a_n] = [a_0, \cdots, a_{n-1}+1].$$

故一有理數必有二種表法，一之 n 爲奇，他之 n 爲偶． 若 α 非有理數，則上法得出一數列

$$a_0, a_1, a_2, \cdots, a_n, \cdots.$$

如

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 21, 31, 14, 2, 1, 2, 2, 2, 2, 1, 84, 2, 1, 1, 15, 3, 13, 1, 4, 2, 6, 6, 1, \cdots].$$

定理 5. 命

$$\alpha_n = [a_0, a_1, \cdots, a_n],$$

則 α_n 之極限存在．

證： 因 $\alpha_n = p_n/q_n$，由定理 3 (ii) 已知

$$\alpha_{2n+1} < \alpha_{2n-1}, \qquad \alpha_{2n} > \alpha_{2n-2}.$$

故 α_{2n+1} 成一遞減之數列，而 α_{2n} 爲一遞增之數列． 又由定理 2 (1) 可知

$$\alpha_1 \geqslant \alpha_{2n+1} \geqslant \alpha_{2n} \geqslant \alpha_2.$$

故 α_{2n} 之限存在，α_{2n+1} 之限亦存在． 更由定理 2 及定理 3 (i) 可知當 $n \to \infty$ 時

$$|\alpha_{2n} - \alpha_{2n-1}| = \frac{1}{q_{2n}\, q_{2n-1}} \leqslant \frac{1}{2n(2n-1)} \to 0.$$

故

$$\lim_{n\to\infty} \alpha_{2n} = \lim_{n\to\infty} \alpha_{2n-1}.$$

習題 1. 求證

$$p_n = \begin{vmatrix} a_0 & -1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & a_1 & -1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & a_2 & -1 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & a_{n-1} & -1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & a_n \end{vmatrix},$$

並證明 q_n 爲由上行列式中除去第一行第一列後之行列式之數值．

習題 2. 員 $\{u_n\}$:

$$1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ \cdots$$

$(u_1 = u_2 = 1,\ u_{i+1} = u_{i-1} + u_i\ (i > 1))$ 稱之爲 Fibonacci 貫. 試證明

(i) $\frac{1}{2}(1+\sqrt{5})$ 之第 n 個漸近分數爲 $\frac{u_{n+2}}{u_{n+1}}$;

(ii) 若連分數 $[a_0, a_1, \cdots, a_n, \cdots]$ 之諸 a_n 中除 $a_i = 2\ (i > 0)$ 外,所有之 $a_n\ (i \neq n)$ 皆等於 1, 則當 $m > i$ 時有

$$\frac{p_m}{q_m} = \frac{u_{i+1}u_{m-i+3} + u_i u_{m-i+1}}{u_i u_{m-i+3} + u_{i-1}u_{m-i+1}}.$$

習題 3. 吾人知道, 朔望月就是從太陽上來看月球繞地球一週所需的時間,也就是相同的月面位相間相隔的時間, 它等於 29.5306 日. 交點月, 就是月球在它軌道上從"交點"開始繞地球一週再回到這個"交點"所需的時間 (所謂"交點"就月球繞地球軌道跟地球繞太陽軌道的交點), 等於 27.2123 日. 試證日,月蝕之週期爲 18 年又 10 天.

習題 4. 火星最亮和離地球最近的一年,叫做火星的大衝. 吾人知道地球公轉一週的週期是 $365\frac{1}{4}$ 日, 火星是 687 日. 試證火星的大衝每隔 15 年一次.

§ 2. 連分數展開之唯一性.

定義. $\alpha'_n = [a_n, a_{n+1}, \cdots]$ 稱爲連分數 $[a_0, a_1, \cdots, a_n, \cdots]$ 之第 $n+1$ 個完全商 (complete quotient).

定理 1. $\alpha = \alpha'_0$, $\alpha = \frac{\alpha'_1 a_0 + 1}{\alpha'_1}$, $\alpha = \frac{\alpha'_n p_{n-1} + p_{n-2}}{\alpha'_n q_{n-1} + q_{n-2}}$, $n \geqslant 2$.
若 α 爲有理數,此式之眞實性止於 N.

證: 當 $n = 2$, 此式顯然. 當 $n > 2$, 因

$$\alpha'_{n-1} = [a_{n-1}, \alpha'_n], \quad \text{卽} \quad \alpha'_{n-1} = a_{n-1} + \frac{1}{\alpha'_n}.$$

故由歸納法之假定,

$$\alpha = \frac{\alpha'_{n-1}p_{n-2} + p_{n-3}}{\alpha'_{n-1}q_{n-2} + q_{n-3}} = \frac{\left(a_{n-1} + \frac{1}{\alpha'_n}\right)p_{n-2} + p_{n-3}}{\left(a_{n-1} + \frac{1}{\alpha'_n}\right)q_{n-2} + q_{n-3}} =$$

$$= \frac{(a_{n-1}p_{n-2} + p_{n-3})\alpha'_n + p_{n-2}}{(a_{n-1}q_{n-2} + q_{n-3})\alpha'_n + q_{n-2}} = \frac{p_{n-1}\alpha'_n + p_{n-2}}{q_{n-1}\alpha'_n + q_{n-2}}.$$

定理 2. 常有

$$a_n = [\alpha'_n].$$

但若 α 爲有理數時,則有一例外,卽當 $a_N = 1$ 時,$a_{N-1} = [\alpha'_{N-1}] - 1$. 由此可見表有理數爲簡單連分數之法唯有兩種.

證: 吾人有次式:

$$\alpha'_n = a_n + \frac{1}{\alpha'_{n+1}}.$$

若 α 非有理數,或 α 爲有理數而 $n \neq N-1$, 則 $\alpha'_{n+1} > 1$, 卽

$$a_n < \alpha'_n < a_n + 1.$$

故得所證. 若 α 爲有理數而 $n = N-1$, 且 $\alpha'_{n+1} = 1$, 則

$$a_n = [\alpha'_n] - 1.$$

定理 3. 用簡單連分數表無理數*之法唯一.

證: 假定

$$\alpha = [a_0, a_1, a_2, \cdots] = [b_0, b_1, b_2, \cdots].$$

顯然可得 $a_0 = [\alpha] = b_0$ 同理可證 $a_1 = b_1$, 今設 $a_0 = b_0$, $a_1 = b_1, \cdots, a_{n-1} = b_{n-1}$ 而往證 $a_n = b_n$. 由

$$\alpha = [a_0, \cdots, a_{n-1}, \alpha'_n] = [a_0, \cdots, a_{n-1}, \beta'_n],$$

可得

$$\alpha = \frac{\alpha'_n p_{n-1} + p_{n-2}}{\alpha'_n q_{n-1} + q_{n-2}} = \frac{\beta'_n p_{n-1} + p_{n-2}}{\beta'_n q_{n-1} + q_{n-2}},$$

卽

$$(\alpha'_n - \beta'_n)(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) = 0.$$

由定理 1.2 可得

$$\alpha'_n = \beta'_n.$$

故

$$a_n = [\alpha'_n] = [\beta'_n] = b_n.$$

---

*) 本章中所謂無理數乃指實數之非有理數者.

定理 4. 吾人有

$$q_n\alpha - p_n = \frac{(-1)^n\delta_n}{q_{n+1}}, \qquad 0 < \delta_n < 1.$$

(若 α 爲有理數，此式祇當 $1 \leqslant n \leqslant N-2$ 時爲眞，而 $\delta_{N-1}=1$)，且 δ_n/q_{n+1} 爲一遞減函數。

證： 已知

$$\alpha = \frac{\alpha'_{n+1}p_n + p_{n-1}}{\alpha'_{n+1}q_n + q_{n-1}},$$

故

$$\alpha - \frac{p_n}{q_n} = \frac{\alpha'_{n+1}p_n + p_{n-1}}{\alpha'_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} =$$

$$= \frac{-(p_nq_{n-1} - q_np_{n-1})}{q_n(\alpha'_{n+1}q_n + q_{n-1})} = \frac{(-1)^n}{q_n(\alpha'_{n+1}q_n + q_{n-1})},$$

故

$$\delta_n = \frac{q_{n+1}}{\alpha'_{n+1}q_n + q_{n-1}} = \frac{a_{n+1}q_n + q_{n-1}}{\alpha'_{n+1}q_n + q_{n-1}}.$$

由此可見，舍 $a_{n+1} = \alpha'_{n+1}$ 之情況外，

$$0 < \delta_n < 1.$$

又因 $\alpha'_n = a_n + 1/\alpha'_{n+1}$，可知

$$\frac{\delta_n}{q_{n+1}} = \frac{1}{\alpha'_{n+1}q_n + q_{n-1}} \geqslant \frac{1}{(a_{n+1}+1)q_n + q_{n-1}} = \frac{1}{q_{n+1}+q_n} \geqslant$$

$$\geqslant \frac{1}{a_{n+2}q_{n+1} + q_n} = \frac{1}{q_{n+2}} \geqslant \frac{\delta_{n+1}}{q_{n+2}}.$$

最後一不等式中，等號僅當 $a_{n+1} = \alpha'_{n+1}$，即 α 爲有理數，$n = N-1$ 時成立。故得定理。

由此定理立可推出：

定理 5. 若 α 爲無理數，則

$$\lim_{n\to\infty} \frac{p_n}{q_n} = \alpha.$$

定理 6. $\left|\alpha - \dfrac{p_n}{q_n}\right| \leqslant \dfrac{1}{q_nq_{n+1}} < \dfrac{1}{q_n^2}.$

祇當 α 爲有理數及 $n = N-1$ 時，取等號。

§ 3. 最佳漸近分數.

在分母不大於 N 之諸有理數中，孰與 α 最爲接近？最接近之分數名爲 α 之最佳漸近分數. 今往證 p_n/q_n 卽爲 α 之最佳漸近分數.

定理 1. 設 $n \geqslant 1$, $0 < q \leqslant q_n$, 且 $p/q \neq p_n/q_n$, 則

$$\left|\frac{p_n}{q_n} - \alpha\right| < \left|\frac{p}{q} - \alpha\right|.$$

故在分母不大於 q_n 之諸分數中,以 p_n/q_n 與 α 最接近.

證: 若能證明

$$|p_n - q_n\alpha| < |p - q\alpha|,$$

則定理已明.

(i) 設 $\alpha = [\alpha] + \frac{1}{2}$. 此時 $\frac{p_1}{q_1} = \alpha$, 故結論顯然成立.

(ii) $\alpha < [\alpha] + \frac{1}{2}$,此結論對 $n = 0$ 時,顯然眞確;$\alpha > [\alpha] + \frac{1}{2}$, 此結論對 $n = 1$ 眞確; 今假定此結論對 $n-1$ 眞確,而用歸納法證明此結論.

若 $q \leqslant q_{n-1}$, 則由歸納法假定

$$|p_{n-1} - q_{n-1}\alpha| < |p - q\alpha|,$$

故可假定 $q_n \geqslant q > q_{n-1}$.

若 $q = q_n$, 則

$$\left|\frac{p_n}{q_n} - \frac{p}{q}\right| \geqslant \frac{1}{q_n}, \qquad p \neq p_n.$$

又

$$\left|\frac{p_n}{q_n} - \alpha\right| \leqslant \frac{1}{q_n q_{n+1}} \leqslant \frac{1}{2q_n}.$$

若 $q_{n+1} = 2$, 則必 $n = 1$. 此時 $a_1 = a_2 = 1$,

$$\alpha = a_0 + \frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{a_3+}\cdots,$$

故必 $a_0 + \frac{1}{2} < \alpha < a_0 + 1$. 我們的結論顯然眞實,故可假定 $q_{n+1} > 2$. 卽

$$\left|\frac{p_n}{q_n} - \alpha\right| \leqslant \frac{1}{q_n q_{n+1}} < \frac{1}{2q_n}.$$

由是得

$$\left|\frac{p}{q} - \alpha\right| \geqslant \left|\frac{p}{q} - \frac{p_n}{q_n}\right| - \left|\frac{p_n}{q_n} - \alpha\right| \geqslant \frac{1}{q_n} - \left|\frac{p_n}{q_n} - \alpha\right| > \left|\frac{p_n}{q_n} - \alpha\right|.$$

故今可假定 $q_n > q > q_{n-1}$. 我們寫

$$up_n + vp_{n-1} = p, \qquad uq_n + vq_{n-1} = q,$$

則

$$u(p_n q_{n-1} - p_{n-1} q_n) = pq_{n-1} - qp_{n-1}.$$

由定理 1.2 得

$$u = \pm(pq_{n-1} - qp_{n-1}),$$

同法

$$v = \pm(pq_n - qp_n),$$

此 u 及 v 皆非爲零,因

$$q_n > q = uq_n + vq_{n-1}.$$

故 u 及 v 一正一負. 又由定理 2.4,

$$p_n - q_n\alpha, \qquad p_{n-1} - q_{n-1}\alpha$$

異號. 故

$$u(p_n - q_n\alpha), \qquad v(p_{n-1} - q_{n-1}\alpha)$$

同號. 由

$$p - q\alpha = u(p_n - q_n\alpha) + v(p_{n-1} - q_{n-1}\alpha)$$

可知

$$|p - q\alpha| > |p_{n-1} - q_{n-1}\alpha| > |p_n - q_n\alpha|.$$

例. 作 $\pi = [3,7,15,1,292,1,1,\cdots]$ 之漸近分數得

$$\frac{3}{1}, \frac{22}{7}, \frac{333}{106}, \frac{355}{113}, \frac{103993}{33102}, \frac{104348}{33215}, \cdots.$$

徑一周三,見諸古籍. 於紀元 500 年頃,祖冲之作疎率 $\frac{22}{7}$ 及密率 $\frac{355}{113}$ (此率較西洋最早之 Otto 紀錄早千年之譜). 最有趣味者,祖氏二率皆屬於最佳漸近分數之列,換言之: 分母不超過 113 之分數,無數比 $\frac{335}{113}$ 更接近於 π 者.

因定理 2.6 可知

$$\left|\pi - \frac{355}{113}\right| < \frac{1}{113\times 33102} < \frac{1}{10^6}.$$

故 $\frac{355}{113}$ 準至第六位小數,此與實際計算之結果 $\frac{355}{113} = 3.1415929$ 相吻合.

§4. Hurwitz 定理.

定理 1. 於 α 之二連續漸近分數中至少有一適合

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{2q^2}.$$

證: 由定理 2.4 可知: $\frac{p_{n+1}}{q_{n+1}}$ 及 $\frac{p_n}{q_n}$ 中一較 α 爲大，一較 α 爲小。故

$$\left|\frac{p_{n+1}}{q_{n+1}}-\frac{p_n}{q_n}\right|=\left|\frac{p_n}{q_n}-\alpha\right|+\left|\frac{p_{n+1}}{q_{n+1}}-\alpha\right|.$$

若定理不眞實，則有

$$\frac{1}{q_n q_{n+1}}=\left|\frac{p_{n+1}}{q_{n+1}}-\frac{p_n}{q_n}\right|\geqslant\frac{1}{2q_n^2}+\frac{1}{2q_{n+1}^2},$$

卽

$$(q_{n+1}-q_n)^2\leqslant 0,$$

此不可能 (若 $n>0$). 故得定理.

由此定理可得: 若 α 爲無理數，必有無窮個 p/q 使

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{2q^2}.$$

定理 2 (Hurwitz). 於 α 之三個連續漸近值中必有一適合

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{\sqrt{5}q^2}.$$

證: 命 $\frac{q_{n-1}}{q_n}=\beta_{n+1}$，則由定理 2.1

$$\left|\frac{p_n}{q_n}-\alpha\right|=\frac{1}{q_n(\alpha'_{n+1}q_n+q_{n-1})}=\frac{1}{q_n^2(\alpha'_{n+1}+\beta_{n+1})}.$$

今往證明，不能有三個連續數 $i=n-1,\ n,\ n+1$ 使

$$\alpha'_i+\beta_i\leqslant\sqrt{5}, \tag{1}$$

今假定 (1) 式當 $i=n-1$ 及 $i=n$ 爲眞實，由

$$\alpha'_{n-1}=a_{n-1}+\frac{1}{\alpha'_n}, \tag{2}$$

及

$$\frac{1}{\beta_n}=\frac{q_{n-1}}{q_{n-2}}=\frac{a_{n-1}q_{n-2}+q_{n-3}}{q_{n-2}}=a_{n-1}+\beta_{n-1},$$

故

$$\frac{1}{\alpha_n'}+\frac{1}{\beta_n}=\alpha_{n-1}'+\beta_{n-1}\leqslant\sqrt{5},$$

立得

$$1=\frac{1}{\alpha_n'}\alpha_n'\leqslant\left(\sqrt{5}-\frac{1}{\beta_n}\right)(\sqrt{5}-\beta_n),$$

卽

$$\beta_n+\frac{1}{\beta_n}\leqslant\sqrt{5}. \tag{3}$$

因 β_n 爲有理數,故不能取等號. 卽得

$$\beta_n^2-\sqrt{5}\,\beta_n+1<0,$$

卽

$$\left(\beta_n-\frac{\sqrt{5}}{2}\right)^2<\frac{1}{4}.$$

因 $\beta_n<1$, 故

$$\beta_n>\frac{1}{2}(\sqrt{5}-1). \tag{4}$$

同法: 若 (1) 式對 $i=n$, $i=n+1$ 爲眞,則有

$$\beta_{n+1}>\frac{1}{2}(\sqrt{5}-1). \tag{5}$$

由 (3), (4), (5) 各式可知

$$a_n=\frac{1}{\beta_{n+1}}-\beta_n<\sqrt{5}-\beta_{n+1}-\beta_n<\sqrt{5}-(\sqrt{5}-1)=1$$

此不可能,故得定理.

由此定理,可立卽推得:

定理 3. 任一無理數 α 有無窮個漸近分數使

$$\left|\frac{p}{q}-\alpha\right|<\frac{1}{\sqrt{5}q^2}.$$

定理 4. $\sqrt{5}$ 乃一至佳之數. 換言之,若 $A>\sqrt{5}$, 則必有一實數 α 使

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{Aq^2}$$

不能有無窮個解.

證: $\alpha=\frac{1}{2}(\sqrt{5}-1)$ 卽其例也. 若不然,設

$$\frac{1}{2}(\sqrt{5}-1)=\frac{p}{q}+\frac{\delta}{q^2},\qquad |\delta|<\frac{1}{A}<\frac{1}{\sqrt{5}},$$

則

$$\frac{\delta}{q}-\frac{1}{2}\sqrt{5}\,q=-\frac{1}{2}q-p.$$

平方此式可得

$$\frac{\delta^2}{q^2}-\sqrt{5}\,\delta=\left(\frac{1}{2}q+p\right)^2-\frac{5}{4}q^2=pq-q^2+p^2.$$

當 q 充分大,則

$$\left|\frac{\delta^2}{q^2}-\sqrt{5}\,\delta\right|<1.$$

故整數

$$pq-q^2+p^2=0,$$

即

$$(2p+q)^2=5q^2.$$

此乃不可能者.

§5. 實數之相似.

定義 1. 若 ξ 與 η 爲二實數,且

$$\xi=\frac{a\eta+b}{c\eta+d},\qquad ad-bc=\pm1,\qquad a,b,c,d \text{ 爲整數}, \tag{1}$$

則 ξ 與 η 謂之相似. 此種由 η 而 ξ 之關係,謂之模變形.

例 1. $\xi=a+\eta$, $\eta=\dfrac{1}{\xi}$ 皆爲模變形.

例 2. $\xi=[a,\zeta]=a+\dfrac{1}{\zeta}$ 亦爲模變形.

例 3. $\alpha=[a_0,a_1,\cdots,a_n,\alpha_n']$ 可以看成爲例二所述之模變形之 n 次連續運用. 而得出之模變形爲

$$\alpha=\frac{p_{n-1}\alpha_n'+p_{n-2}}{q_{n-1}\alpha_n'+q_{n-2}}.$$

關於相似性有次之諸性質:

(i) 一數必與其自身相似. 蓋 $\xi=\eta$ 是一模變形 $(a=d=1,\ b=c=0)$ 也.

(ii) 若 ξ 與 η 相似,則 η 與 ξ 亦相似. 蓋由 (1) 式,可得 $\eta=(d\xi-b)/(-c\xi+a)$,而此亦一模變形也.

(iii) 若 ξ 與 η 相似，η 與 ζ 相似，則 ξ 與 ζ 相似. 蓋若 $\xi=(a\eta+b)/(c\eta+d)$, $\eta=(a_1\zeta+b_1)/(c_1\zeta+d_1)$, 則

$$\xi=\{(aa_1+bc_1)\zeta+(ab_1+bd_1)\}/\{(ca_1+dc_1)\zeta+(cb_1+dd_1)\},$$

此處

$$(aa_1+bc_1)(cb_1+dd_1)-(ab_1+bd_1)(ca_1+dc_1)=(ad-bc)(a_1d_1-b_1c_1)=\pm 1.$$

定義 2. (iii) 中最後得出之模變形稱爲前二模變形之積.

定理 1. 凡有理數必相似.

證: 設 p/q, $(p,q)=1$ 爲一有理數，則有 p' 及 q' 使

$$pq'-qp'=1.$$

故

$$\frac{p}{q}=\frac{p'\cdot 0+p}{q'\cdot 0+q}=\frac{a\cdot 0+b}{c\cdot 0+d},\qquad ad-bc=-1.$$

卽有理數都相似於 0，故得定理.

定理 2. 模變形 (1) 可以表成爲連分數之形式

$$\xi=[a_0,a_1,\cdots,a_{k-1},\eta],\qquad k\geqslant 2 \tag{2}$$

的必要且充分之條件爲有二整數 c 與 d，滿足

$$c>d>0. \tag{3}$$

證: 1) 由 (2) 可得

$$\xi=(p_{k-1}\eta+p_{k-2})/(q_{k-1}\eta+q_{k-2}),$$

此顯然適合條件 (3).

2) 今對 d 行歸納法以證明定理之逆部分.

當 $d=1$，則 $a=bc\pm 1$，卽

$$\xi=((bc\pm 1)\eta+b)/(c\eta+1).$$

若取正號，則

$$\xi=b+\frac{\eta}{c\eta+1}=[b,c,\eta].$$

若取負號，則

$$\xi=b-1+\frac{(c-1)\eta+1}{c\eta+1}=[b-1,1,c-1,\eta].$$

由於

$$\xi=(b\zeta+a-bq)/(d\zeta+c-dq) \tag{4}$$

與

$$\zeta=[q,\eta]=q+\frac{1}{\eta}$$

之積等於 (1) 式. 如取 q 使 $0<c-dq<d$ (因 $d>1$, $(c, d)=1$), 則 (4) 式中對應於 d 之元素小於 d, 故得定理.

定理 3. 二無理數相似之必要且充分之條件爲

$$\xi=[a_0, a_1, \cdots, a_m, c_0, c_1, \cdots],$$
$$\eta=[b_0, b_1, \cdots, b_n, c_0, c_1, \cdots].$$

換言之,其連分數之展開式中,自若干項之後完全相同.

證: 1) 命 $\omega=[c_0, c_1, \cdots]$, 則

$$\xi=[a_0, a_1, \cdots, a_m, \omega]=\frac{\omega p_m+p_{m-1}}{\omega q_m+q_{m-1}}, \quad p_m q_{m-1}-q_m p_{m-1}=\pm 1.$$

故 ω 與 ξ 相似. 同法 ω 與 η 相似,故 ξ 與 η 相似.

2) 若 ξ 與 η 相似,則

$$\eta=(a\xi+b)(c\xi+d)^{-1}, \quad ad-bc=\pm 1.$$

可以假定 $c\xi+d>0$. 展開 ξ 爲連分數:

$$\xi=[a_0, \cdots, a_k, a_{k+1}, \cdots]=[a_0, \cdots, a_{k-1}, \alpha_k']=$$
$$=(\alpha_k' p_{k-1}+p_{k-2})(\alpha_k' q_{k-1}+q_{k-2})^{-1}.$$

相併可得

$$\eta=(P\alpha_k'+R)(Q\alpha_k'+S)^{-1},$$

此處 $P=ap_{k-1}+bq_{k-1}$, $R=ap_{k-2}+bq_{k-2}$, $Q=cp_{k-1}+dq_{k-1}$, $S=cp_{k-2}+$ $+dq_{k-2}$, P, Q, R, S 皆爲整數,且適合 $PS-QR=\pm 1$.

由定理 2.4 可知

$$p_{k-1}=\xi q_{k-1}+\frac{\delta}{q_{k-1}}, \quad p_{k-2}=\xi q_{k-2}+\frac{\delta'}{q_{k-2}}, \quad |\delta|<1, |\delta'|<1,$$

故

$$Q=(c\xi+d)q_{k-1}+\frac{c\delta}{q_{k-1}}, \quad S=(c\xi+d)q_{k-2}+\frac{c\delta'}{q_{k-2}}.$$

由 $c\xi+d>0$, 及 $q_{k-2}\geqslant k-2$. $q_{k-1}\geqslant q_{k-2}+1$ (定理 1.3),可知當 k 充分大時,

$$Q>S>0.$$

由定理 2, 可知

$$\eta=[b_0,\cdots,b_n,\alpha'_k].$$

故條件之必要性獲證。

命 $M(\alpha)$ 爲最大之數,使得對任何 $\varepsilon>0$, 不等式

$$\left|\alpha-\frac{p_i}{q_i}\right|\leqslant\frac{1}{(M(\alpha)-\varepsilon)\,q_i^2}$$

有無窮個解答者. 例如: $M\left(\frac{1}{2}(\sqrt{5}-1)\right)=\sqrt{5}$. 命

$$\alpha-\frac{p_i}{q_i}=\frac{1}{\lambda_i\,q_i^2},$$

則

$$\lambda_i=(-1)^i\left(\alpha'_{i+1}+\frac{q_{i-1}}{q_i}\right),\quad \alpha'_{i+1}=[a_{i+1},a_{i+2},\cdots].$$

又

$$\frac{q_{i-1}}{q_i}=\frac{1}{q_i/q_{i-1}}=\frac{1}{a_i}+\frac{q_{i-2}}{q_{i-1}}=\frac{1}{a_i}+\frac{1}{a_{i-1}}+\frac{q_{i-3}}{q_{i-2}}=\cdots=$$
$$=[0,a_i,a_{i-1},\cdots,a_2,a_1].$$

故

$$M(\alpha)=\overline{\lim_{i\to\infty}}\,\lambda_i=\overline{\lim_{i\to\infty}}\,([a_{i+1},a_{i+2},\cdots]+$$
$$+[0,a_i,a_{i-1},\cdots,a_2,a_1]).$$

若 α 與 β 相似,則當 i 充分大時 $a_i=b_i$ 故可得:

定 理 4. 若 α 與 β 相似,則

$$M(\alpha)=M(\beta).$$

由此可得: 若 α 與 $\frac{1}{2}(\sqrt{5}-1)$ 相似,則適合

$$\left|\frac{p}{q}-\alpha\right|<\frac{1}{Aq^2},\qquad A>\sqrt{5}$$

之解數有限. 進言之,若 α 不與 $\frac{1}{2}(\sqrt{5}-1)$ 相似, 則 $M(\alpha)$ 之情況何如?

吾人有次之結果:

若 α 不與 $\frac{1}{2}(\sqrt{5}-1)$ 相似,則 $M(\alpha) \geqslant \sqrt{8}$. 切實言之,對此種之 α

$$\left|\frac{p}{q}-\alpha\right| < \frac{1}{\sqrt{8}\,q^2}$$

有無窮個解.

又若 α 與 $1+\sqrt{2}$ 相似,則 $M(\alpha)=\sqrt{8}$. 普遍言之,可有次之結果:

定義. u 爲一自然數,如

$$u^2+v^2+w^2=3uvw$$

有整數解 (v, w) 則此 u 名爲 Марков 數. 最初之十個 Марков 數爲

$$1, 2, 5, 13, 29, 34, 89, 169, 194, 233, 433, \cdots$$

(Марков 數之個數無窮,將於次章證明之).

若 α 與

$$\frac{1}{2u}\left(\sqrt{9u^2-4}+u+\frac{2v}{w}\right)=\alpha_u$$

相似,則 $M(\alpha_u)=\dfrac{\sqrt{9u^2-4}}{u}$, 此處之 u 爲 Марков 數, v 及 w 爲對應之解,且若 α 不與 $\alpha_u (1 \leqslant u \leqslant v)$ 相似,則

$$\left|\alpha-\frac{p}{q}\right| < \frac{1}{M(\alpha_v)\,q^2}$$

有無窮個解.

由此可見,若 α 非具有理係數的二次方程之根,則對任一 u 常有

$$M(\alpha) \geqslant \frac{\sqrt{9u^2-4}}{u}.$$

當此 u 趨向無窮,則

$$M(\alpha) \geqslant 3.$$

又若 $0 < m_1 < m_2 < \cdots$, 則

$$\alpha=[2, 2, \underbrace{1, 1, \cdots, 1}_{m_1}, 2, 2, \underbrace{1, \cdots, 1}_{m_2}, 2, 2, \underbrace{1, 1, \cdots, 1}_{m_3}, \cdots]$$

乃適合 $M(\alpha)=3$ 之數,以上所述之結果之證明不在此書範圍之內.

§ 6. 循環連分數.

定義. 當 $l \geqslant L$ 時, 若 $a_l = a_{l+k}$, 則此連分數, 謂之循環連分數, 或謂以 k 爲週期之循環連分數, 書作

$$[a_0, \cdots, a_{L-1}, \dot{a}_L, \cdots, \dot{a}_{L+k-1}].$$

先舉數例:

$$\sqrt{2} = 1 + (\sqrt{2} - 1) = 1 + \frac{1}{\sqrt{2}+1} = 1 + \frac{1}{2+(\sqrt{2}-1)} =$$

$$= 1 + \frac{1}{2} + \frac{1}{2} + \cdots = [1, \dot{2}].$$

$$\sqrt{3} = 1 + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \frac{1}{2} + \cdots = [1, \dot{1}, \dot{2}].$$

$$\sqrt{5} = [2, \dot{4}], \qquad \sqrt{7} = [2, \dot{1}, 1, 1, \dot{4}].$$

此建議:

定理 1. 一連分數爲循環連分數之必要且充分條件爲此數爲一有有理係數之二次不可化方程式之根.

證: 1) 命

$$\alpha'_L = [\dot{a}_L, \cdots, \dot{a}_{L+k-1}] = [a_L, \cdots, a_{L+k-1}, \alpha'_L],$$

卽得

$$\alpha'_L = \frac{p'\alpha'_L + p''}{q'\alpha'_L + q''},$$

故 α'_L 適合

$$q'\alpha'^2_L + (q'' - p')\alpha'_L - p'' = 0.$$

(式中 p''/q'', p'/q' 爲 $[a_L, \cdots, a_{L+k-1}]$ 之最後二漸近分數), 又

$$\alpha = (p_{L-1}\alpha'_L + p_{L-2}) / (q_{L-1}\alpha'_L + q_{L-2}).$$

故知 α 適合

$$a\alpha^2 + b\alpha + c = 0.$$

因 α 爲無理數, 故 $b^2 - 4ac$ 非一完全平方.

2) 設 α 適合

$$a\alpha^2 + b\alpha + c = 0.$$

命

$$\alpha = [a_0, a_1, \cdots, a_n, \cdots],$$

則

$$\alpha = (p_{n-1}\alpha'_n + p_{n-2}) / (q_{n-1}\alpha'_n + q_{n-2}).$$

以此代入上式，則得

$$A_n \alpha'^2_n + B_n \alpha'_n + C_n = 0,$$

式中

$$A_n = ap^2_{n-1} + bp_{n-1}q_{n-1} + cq^2_{n-1},$$

$$B_n = 2ap_{n-1}p_{n-2} + b(p_{n-1}q_{n-2} + p_{n-2}q_{n-1}) + 2cq_{n-1}q_{n-2},$$

$$C_n = ap^2_{n-2} + bp_{n-2}q_{n-2} + cq^2_{n-2}.$$

若 $A_n = 0$，則 $a\alpha^2 + b\alpha + c = 0$ 有有理根，是不可能，故 $A_n \neq 0$，且

$$A_n y^2 + B_n y + C_n = 0$$

之一根為 α'_n. 直接計算可得

$$B^2_n - 4A_nC_n = (b^2 - 4ac)(p_{n-1}q_{n-2} - p_{n-2}q_{n-1})^2 = (b^2 - 4ac).$$

由定理 2.4,

$$p_{n-1} = \alpha q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}, \qquad |\delta_{n-1}| < 1.$$

故

$$A_n = a\left(\alpha q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}\right)^2 + b q_{n-1}\left(\alpha q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}\right) + c q^2_{n-1} =$$

$$= (a\alpha^2 + b\alpha + c) q^2_{n-1} + 2a\alpha\delta_{n-1} + a\frac{\delta^2_{n-1}}{q^2_{n-1}} + b\delta_{n-1} =$$

$$= 2a\alpha\delta_{n-1} + a\frac{\delta^2_{n-1}}{q^2_{n-1}} + b\delta_{n-1}.$$

由此立得

$$|A_n| < 2|a\alpha| + |a| + |b|.$$

因 $C_n = A_{n-1}$，故

$$|C_n| < 2|a\alpha| + |a| + |b|.$$

再由

$$B^2_n \leqslant 4|A_nC_n| + |b^2 - 4ac| < 4(2|a\alpha| + |a| + |b|)^2 + |b^2 - 4ac|.$$

故 A_n, B_n, C_n 之絕對值小於與 n 無關之數，即祇有有限組 (A_n, B_n, C_n). 故

至少有同一 (A_n, B_n, C_n) 出現三次. 設 $n=n_1, n_2, n_3$ 對應同一組 (A_n, B_n, C_n), 則 $\alpha'_{n_1}, \alpha'_{n_2}, \alpha'_{n_3}$ 爲

$$A_n y^2 + B_n y + C_n = 0$$

之根. 故至少有二者相等. 設 $\alpha'_{n_1} = \alpha'_{n_2}$ 則

$$a_{n_1} = a_{n_2}, \quad a_{n_1+1} = a_{n_2+1}, \cdots,$$

故連分數是循環的.

§ 7. **Legendre 之判斷條件.**

由前已知,若 $\frac{p}{q}$ 是 α 的一個漸近值,則

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

但此並不保證 $\frac{p}{q}$ 爲 α 之漸近值,今往求一保證 $\frac{p}{q}$ 爲 α 之一漸近分數之必要且充分之條件. 命

$$\alpha - \frac{p}{q} = \frac{\epsilon\vartheta}{q^2}, \quad \epsilon = \pm 1, \quad 0 < \vartheta < 1.$$

命

$$\frac{p}{q} = [a_0, \cdots, a_{n-1}] = \frac{p_{n-1}}{q_{n-1}}.$$

當可取 n 使 $(-1)^{n-1} = \epsilon$. 原式可寫做

$$\alpha - \frac{p_{n-1}}{q_{n-1}} = \frac{\epsilon\vartheta}{q_{n-1}^2}.$$

由次式以定義 β:

$$\alpha = \frac{p_{n-1}\beta + p_{n-2}}{q_{n-1}\beta + q_{n-2}}, \tag{1}$$

如是則

$$\frac{\epsilon\vartheta}{q_{n-1}^2} = \frac{p_{n-1}\beta + p_{n-2}}{q_{n-1}\beta + q_{n-2}} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_{n-1}(q_{n-1}\beta + q_{n-2})}.$$

故

$$\vartheta = \frac{q_{n-1}}{q_{n-1}\beta + q_{n-2}}.$$

解此式可得

$$\beta = (q_{n-1} - \vartheta q_{n-2}) / (\vartheta q_{n-1})$$

因 $0 < \vartheta < 1$, 故 $\beta > 0$.

(1) 式即謂

$$\alpha=[a_0,\cdots,a_{n-1},\beta].$$

若 $\beta\geqslant 1$, 則

$$\beta=\alpha_n'\,(=[a_n,a_{n+1},\cdots]).$$

即 $p/q=p_{n-1}/q_{n-1}$ 爲 α 之漸近值.

若 $\beta<1$, 因 $\beta>0$, 可知

$$\left[a_{n-1}+\frac{1}{\beta}\right]=a_{n-1}+c,\qquad c>0.$$

即

$$\alpha=[a_0,\cdots,a_{n-2},a_{n-1}+c,\cdots].$$

即 $[a_0,\cdots,a_{n-1}]$ 非 α 之漸近值. 是以 $\beta\geqslant 1$ 爲必要且充分之條件,換言之:

定理 1 (Legendre). 命

$$\epsilon\vartheta=q^2\alpha-pq,\qquad \epsilon=\pm 1,\qquad 0<\vartheta<1.$$

展開

$$\frac{p}{q}=[a_0,\cdots,a_{n-1}],\qquad (-1)^{n-1}=\epsilon,$$

則 $\frac{p}{q}$ 爲 α 之漸近值之必要且充分之條件爲

$$\vartheta\leqslant\frac{q_{n-1}}{q_{n-1}+q_{n-2}}$$

(此卽 $\beta\geqslant 1$ 之改書也).

因

$$\frac{q_{n-1}}{q_{n-1}+q_{n-2}}>\frac{1}{2},$$

故立得:

定理 2. 若有一有理數 p/q 適合

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{2q^2},$$

則 p/q 必爲 α 之一漸近值.

定理 3. 若 $p>0$, $q>0$, 且

$$|p^2-\alpha^2q^2|<\alpha,$$

則 p/q 必爲 α 之一漸近值.

證: 命

$$\alpha^2 q^2 - p^2 = \epsilon\,\delta\alpha, \qquad \epsilon = \pm 1, \qquad 0 \leqslant \delta < 1,$$

則

$$\alpha q - p = \frac{\epsilon\,\delta\alpha}{\alpha q + p},$$

故

$$\vartheta = \epsilon q(\alpha q - p) = \frac{\delta\alpha q}{\alpha q + p} = \frac{\delta\alpha\, q_{n-1}}{\alpha q_{n-1} + p_{n-1}}, \qquad (-1)^{n-1} = \epsilon.$$

由定理 1 可知祇須證明

$$\frac{\delta\alpha\, q_{n-1}}{\alpha q_{n-1} + p_{n-1}} < \frac{q_{n-1}}{q_{n-1} + q_{n-2}},$$

亦卽求證

$$\delta\alpha(q_{n-1} + q_{n-2}) < \alpha q_{n-1} + p_{n-1}$$

(當 $n = 2$, 此式顯然眞確,蓋 $\delta < 1$, $\delta\alpha q_0 = \delta\alpha < \alpha < p_1$ 故也). 如能證明下式,當已足够:

$$\alpha q_{n-1} - p_{n-1} < \alpha(q_{n-1} - q_{n-2}), \qquad n > 2,$$

因

$$\alpha q_{n-1} - p_{n-1} = \frac{\epsilon\,\delta\,\alpha}{\alpha q_{n-1} + p_{n-1}},$$

故如能證明

$$\frac{\epsilon\,\delta}{\alpha q_{n-1} + p_{n-1}} < q_{n-1} - q_{n-2}$$

卽足,亦卽如能證明

$$\frac{1}{\alpha q_{n-1} + p_{n-1}} < q_{n-1} - q_{n-2}$$

卽足,而此式無疑眞實,蓋由定理 1.3 已知

$$q_{n-1} - q_{n-2} \geqslant 1 > \frac{1}{\alpha q_{n-1} + p_{n-1}}$$

故也.

§8. 二次不定方程.

玆討論整未知數 x, y 的方程

$$x^2 - dy^2 = l, \qquad 0 < |l| < \sqrt{d}.$$

在本節及下節中我們假定 d 爲正整數,但非整數的平方.

定理 1. 於 $\sqrt{d}$ 之展開式中 α'_n 之形式必爲

$$\frac{\sqrt{d}+P_n}{Q_n}, \qquad P_n^2 \equiv d \qquad (\bmod Q_n),$$

此處 P_n 及 Q_n 皆爲整數.

證: 今用歸納法: 顯然

$$\sqrt{d}-[\sqrt{d}]=\frac{1}{\alpha_1'}, \qquad 即 \qquad \alpha_1'=\frac{\sqrt{d}+[\sqrt{d}]}{d-[\sqrt{d}]^2}.$$

即 $P_1=[\sqrt{d}]$, $Q_1=d-[\sqrt{d}]^2$. 今假定 $\alpha_n'=\dfrac{\sqrt{d}+P_n}{Q_n}$. 因

$$\alpha_n'=a_n+\frac{1}{\alpha_{n+1}'},$$

故所待證者爲: 有二整數 P_{n+1} 及 Q_{n+1} 使

$$\frac{\sqrt{d}+P_n}{Q_n}=a_n+\frac{Q_{n+1}}{\sqrt{d}+P_{n+1}},$$

及

$$d-P_{n+1}^2\equiv 0 \qquad (\bmod Q_{n+1}). \tag{1}$$

亦即需證明: 有二整數 P_{n+1} 及 Q_{n+1} 使

$$d+P_nP_{n+1}=a_nQ_nP_{n+1}+Q_nQ_{n+1}, \tag{2}$$

$$P_n+P_{n+1}=a_nQ_n \tag{3}$$

及 (1) 式. 從 (2) 式減去 (3) 之 P_{n+1} 倍,可得

$$d-P_{n+1}^2=Q_nQ_{n+1}. \tag{4}$$

苟適合 (4),必適合 (1),又由 (3),(4) 可得 (2) 式. 故今祇須證明有二整數 P_{n+1} 及 Q_{n+1} 適合 (3) 及 (4).

由 (3) 式可解得 P_{n+1} 之值. 由 $P_n^2\equiv P_{n+1}^2$ $(\bmod Q_n)$,可知

$$d-P_{n+1}^2\equiv 0 \qquad (\bmod Q_n),$$

故有 Q_{n+1} 存在適合 (4) 式. 故定理業已證明.

定理 2. 二次不定方程

$$x^2-dy^2=(-1)^nQ_n$$

常有解. 若 $l\neq(-1)^nQ_n$, 且 $|l|<\sqrt{d}$ 則

$$x^2-dy^2=l$$

不可解.

證: 已知

$$\sqrt{d} = \frac{p_{n-1}\alpha'_n + p_{n-2}}{q_{n-1}\alpha'_n + q_{n-2}} = \frac{p_{n-1}(\sqrt{d}+P_n)+p_{n-2}Q_n}{q_{n-1}(\sqrt{d}+P_n)+q_{n-2}Q_n},$$

由 $\sqrt{d}$ 爲無理數,故清理分數可得

$$p_{n-1} = q_{n-1}P_n + q_{n-2}Q_n;$$

$$d\,q_{n-1} = p_{n-1}P_n + p_{n-2}Q_n.$$

以 p_{n-1} 乘第一式減去以 q_{n-1} 乘第二式,可得

$$p_{n-1}^2 - d\,q_{n-1}^2 = (p_{n-1}q_{n-2} - p_{n-2}q_{n-1})Q_n = (-1)^n Q_n.$$

定理之其他一半,可由定理 7.3 得之.

定理 3. 若 k 爲 $\sqrt{d}$ 之連分數之週期(即循環節之長),且 $n > L$ 及

$$p_{n-1}^2 - d\,q_{n-1}^2 = (-1)^n Q_n,$$

則

$$p_{n-1+lk}^2 - d\,q_{n-1+lk}^2 = (-1)^{n+lk} Q_n.$$

證: 若 k 爲 $\sqrt{d}$ 之週期,則

$$\frac{\sqrt{d}+P_n}{Q_n} = \frac{\sqrt{d}+P_{n+lk}}{Q_{n+lk}}.$$

故得定理.

§9. Pell 氏方程.

今往解 Pell 氏方程

$$x^2 - d\,y^2 = \pm 1. \tag{1}$$

由定理 8.3 已知必有一 Q 使

$$x^2 - d\,y^2 = Q$$

有無窮個解答. 今依 mod $|Q|$ 分此式之諸解爲 Q^2 類. 必有一類其中至少有二解. 換言之,必有整數 x_1, y_1 及 x_2, y_2 使

$$x_1^2 - d\,y_1^2 = x_2^2 - d\,y_2^2 = Q, \qquad x_1 > 0,\ y_1 > 0,\ x_2 > 0,\ y_2 > 0.$$

且

$$x_1 \equiv x_2 \pmod{|Q|}, \qquad y_1 \equiv y_2 \pmod{|Q|}, \qquad x_1 \neq x_2.$$

今往證

$$x=\frac{x_1 x_2-d y_1 y_2}{Q}, \qquad y=\frac{x_1 y_2-x_2 y_1}{Q}$$

即爲 Pell 氏方程 (1) 之解:

1) x 及 y 皆爲整數. 因爲

$$x_1 x_2-d y_1 y_2 \equiv x_1^2-d y_1^2=Q \equiv 0 \quad (\bmod |Q|),$$

$$x_1 y_2-x_2 y_1 \equiv x_1 y_1-x_1 y_1 \equiv 0 \quad (\bmod |Q|).$$

2) x, y 適合 Pell 氏方程. 因爲

$$Q^2(x^2-d y^2)=(x_1 x_2-d y_1 y_2)^2-d(x_1 y_2-x_2 y_1)^2=$$

$$=(x_1^2-d y_1^2)(x_2^2-d y_2^2)=Q^2.$$

3) (x, y) 非顯然解 $(\pm 1, 0)$, 即 $y \neq 0$. 若不然,

$$x_1 y_2-x_2 y_1=0.$$

由 $(x_1, y_1)=(x_2, y_2)=1$, 故 $x_1=x_2$, $y_1=y_2$ 此與假定相違背.

故可知:

定理 1. Pell 氏方程

$$x^2-d y^2=1$$

有一解 (x, y), $y \neq 0$.

由定理 7.3 得出 $\frac{x}{y}=\frac{p_{n-1}}{q_{n-1}}$ 是 $\sqrt{d}$ 之漸近分數, 故由定理 8.2 得知有一 n 使 $(-1)^n Q_n=1$.

定理 2. 命 n 爲使 $(-1)^n Q_n=1$ 之最小正整數, 則

$$x^2-d y^2=1$$

之諸根, 皆由次式得之

$$x+\sqrt{d}\, y=\pm(p_{n-1}+\sqrt{d}\, q_{n-1})^l, \qquad l \gtreqless 0.$$

證: 命

$$\epsilon=p_{n-1}+\sqrt{d}\, q_{n-1}.$$

顯然可見 $\epsilon>1$, 因

$$\pm \frac{1}{x+\sqrt{d}\, y}=\pm(x-\sqrt{d}\, y),$$

故祇須證明: 凡

$$x^2-dy^2=1 \qquad x>0, \qquad y>0$$

之根 (x, y) 皆可表爲 $x+y\sqrt{d}=\varepsilon^m$ $(m>0)$.

命 (x, y) 爲如此之一根,則

$$x+y\sqrt{d}>1.$$

必有一整數 $m\geqslant 0$ 使

$$\varepsilon^m\leqslant x+y\sqrt{d}<\varepsilon^{m+1}.$$

卽

$$1\leqslant \varepsilon^{-m}(x+y\sqrt{d})<\varepsilon.$$

命

$$\varepsilon^{-m}(x+y\sqrt{d})=(x_0-y_0\sqrt{d})(x+y\sqrt{d})=X+Y\sqrt{d}.$$

因 $\sqrt{d}$ 爲無理數,故

$$(x_0+y_0\sqrt{d})(x-y\sqrt{d})=X-Y\sqrt{d}.$$

相乘得

$$X^2-dY^2=1.$$

今設

$$1<X+\sqrt{d}Y<\epsilon.$$

故

$$0<\epsilon^{-1}<(X+\sqrt{d}Y)^{-1}=X-\sqrt{d}Y<1.$$

相加相減得

$$2X=(X+\sqrt{d}Y)+(X-\sqrt{d}Y)>1+\epsilon^{-1}>0,$$

$$2\sqrt{d}Y=(X+\sqrt{d}Y)-(X-\sqrt{d}Y)>1-1=0.$$

由此可知

$$X^2-dY^2=1, \qquad X>0, \qquad Y>0.$$

且

$$1<X+\sqrt{d}Y<p_{n-1}+\sqrt{d}q_{n-1},$$

因 $x=\sqrt{1+dy^2}$ 隨 y 之增大而增大,故 $x+\sqrt{d}\,y$ 亦隨 y 之增大而增大,故由上式可得 $Y<q_{n-1}$, 且 $X<p_{n-1}$. 卽 $\frac{X}{Y}$ 爲一分母小於 q_{n-1} 之漸近分數,此不可能,故得 $X+Y\sqrt{d}=1$.

以前所述可知 $x^2-dy^2=1$ 常可解,但

$$x^2-dy^2=-1,$$

則不一定常可解．例如 $x^2-3y^2=-1$ 不可解．因 $x^2\equiv 0,1 \pmod 4$，$x^2-3y^2\equiv x^2+y^2\equiv 0,1,2 \pmod 4$，而 $\not\equiv -1 \pmod 4$ 故也．此例顯示若 $d\equiv 3 \pmod 4$，$x^2-dy^2=-1$ 常不可解．

但若有 x_0, y_0 使

$$x_0^2-d\,y_0^2=-1,$$

則由

$$x_1+\sqrt{d}\,y_1=(x_0+\sqrt{d}\,y_0)^2.$$

所定義之 x_1, y_1 適合

$$x_1^2-d\,y_1^2=1.$$

易證：若 $x^2-dy^2=-1$ 有解，則 $x^2-dy^2=\pm 1$ 所有的根可由

$$\pm(p_{n-1}+\sqrt{d}\,q_{n-1})^l$$

表出之，而 n 是使 $(-1)^n Q_n=-1$ 成立的最小正整數．

§10. Чебышев 定理及 Хинчин 定理．

設 ϑ 為一無理實數，定理 4 1 已說明有無窮多對整數 x, y 使

$$|x\vartheta-y|<\frac{1}{x},\qquad (x,y)=1. \tag{1}$$

由此結果，吾人可以立刻引伸出下面的結論：

任與一 $\varepsilon>0$，必有一整數 x 存在，使 $x\vartheta$ 與某一整數之差小於 ε，換言之，點集

$$x\vartheta-[x\vartheta],\qquad x=1,2,3,\cdots \tag{2}$$

以 0 為其一極限點．

這裏自然就會發生求點集 (2) 的所有極限點的問題．關於這一問題，Чебышев 曾證明：(0,1) 之間的任一點皆為點集 (2) 之一極限點，或更精密些，他證明了

定理 1． 設 ϑ 為一無理實數，β 為任一實數，則有無窮對整數 x, y，使

$$|\vartheta x-y-\beta|<\frac{3}{x}. \tag{3}$$

證：由定理 4.1 有無限多對整數 $p, q>0$ 使

$$\vartheta=\frac{p}{q}+\frac{\delta}{q^2},\qquad |\delta|<1,\qquad (p,q)=1. \tag{4}$$

對於固定的 q 及 β，常可求得整數 t，使

$$|q\beta-t|\leqslant\frac{1}{2}.$$

由是

$$\beta=\frac{t}{q}+\frac{\delta'}{2q}\qquad (|\delta'|\leqslant 1). \tag{5}$$

因 $(p,q)=1$，故存在整數對 x,y，使

$$\frac{q}{2}\leqslant x<\frac{3}{2}q,\qquad px-qy=t. \tag{6}$$

由 (4) 及 (5)，有

$$|\vartheta x-y-\beta|=\left|\frac{xp}{q}+\frac{x\delta}{q^2}-y-\frac{t}{q}-\frac{\delta'}{2q}\right|=$$

$$=\left|\frac{x\delta}{q^2}-\frac{\delta'}{2q}\right|<\frac{x}{q^2}+\frac{1}{2q}.$$

因 $q>\frac{2}{3}x$，故得

$$|\vartheta x-y-\beta|<\frac{9}{4x}+\frac{3}{4x}=\frac{3}{x}.$$

因 q 可任意大，而由 (6)，$x\geqslant\frac{q}{2}$．故吾人之定理卽已證明．

定理 1 說明了對於任一無理實數 ϑ 及任一實數 β，存在常數 c，使不等式

$$|\vartheta x-y-\beta|<\frac{c}{x} \tag{7}$$

有無窮對整數解 $x>0$, y．該定理且證明 $c=3$，將此常數 c 予以改善，乃一自然發生的問題．由定理 4.4，我們可以看出 c 必須 $\geqslant\frac{1}{\sqrt{5}}$. Хинчин 曾證明了下面的結果:

定理 2. 設 ϑ 爲一無理實數，β 爲實數，$\varepsilon>0$，則不等式

$$|x\vartheta-y-\beta|<\frac{1+\varepsilon}{\sqrt{5}x} \tag{8}$$

有無窮對整數解 $x>0$, y.

證： 由定理 4.3，吾人有無窮對整數 $p,q,(p,q)=1$ 使 $\vartheta=\frac{p}{q}+\frac{\delta}{q^2}$;

$0<|\delta|<\frac{1}{\sqrt{5}}$. 不妨假定 $\delta>0$, 否則只須以 $(-\vartheta,-\beta)$ 代 (ϑ,β) 卽可. 吾人已知, 若 ξ_1, ξ_2 爲任意二實數 (ξ_1, ξ_2 將在後面決定), $\xi_2-\xi_1\geqslant 1$, 則常可求得整數對 x, y 使

$$px-qy=[q\beta], \qquad \xi_1 q\leqslant x<\xi_2 q. \tag{9}$$

由是

$$|x\vartheta-y-\beta|=\left|\frac{p}{q}x+\frac{\delta x}{q^2}-y-\frac{[q\beta]}{q}-\frac{\tau}{q}\right|=$$

$$=\frac{1}{q}\left|\frac{x\delta}{q}-\tau\right|=\frac{1}{x}\cdot\frac{x}{q}\left|\frac{x\delta}{q}-\tau\right|, \tag{10}$$

於此 $\tau=q\beta-[q\beta]$.

1) 如欲

$$-\frac{1}{\sqrt{5}}\leqslant\frac{x}{q}\left(\frac{x\delta}{q}-\tau\right)<\frac{1}{\sqrt{5}},$$

則必

$$\frac{\tau^2}{4\delta}-\frac{1}{\sqrt{5}}\leqslant\frac{x^2\delta}{q^2}-\frac{x\tau}{q}+\frac{\tau^2}{4\delta}<\frac{\tau^2}{4\delta}+\frac{1}{\sqrt{5}}.$$

若假定

$$\tau^2\geqslant\frac{4\delta}{\sqrt{5}}, \tag{11}$$

則由上式立得

$$\sqrt{\frac{\tau^2}{4\delta}-\frac{1}{\sqrt{5}}}\leqslant\frac{x\sqrt{\delta}}{q}-\frac{\tau}{2\sqrt{\delta}}<\sqrt{\frac{\tau^2}{4\delta}+\frac{1}{\sqrt{5}}}.$$

卽

$$\frac{1}{\sqrt{\delta}}\left(\frac{\tau}{2\sqrt{\delta}}+\sqrt{\frac{\tau^2}{4\delta}-\frac{1}{\sqrt{5}}}\right)\leqslant\frac{x}{q}<\frac{1}{\sqrt{\delta}}\left(\frac{\tau}{2\sqrt{\delta}}+\sqrt{\frac{\tau^2}{4\delta}+\frac{1}{\sqrt{5}}}\right).$$

令

$$\xi_1=\frac{1}{\sqrt{\delta}}\left(\frac{\tau}{2\sqrt{\delta}}+\sqrt{\frac{\tau^2}{4\delta}-\frac{1}{\sqrt{5}}}\right);$$

$$\xi_2=\frac{1}{\sqrt{\delta}}\left(\frac{\tau}{2\sqrt{\delta}}+\sqrt{\frac{\tau^2}{4\delta}+\frac{1}{\sqrt{5}}}\right).$$

我們來研究如何才能使 $\xi_2-\xi_1\geqslant 1$. 將不等式

$$\frac{1}{\sqrt{\delta}}\left(\sqrt{\frac{\tau^2}{4\delta}+\frac{1}{\sqrt{5}}}-\sqrt{\frac{\tau^2}{4\delta}-\frac{1}{\sqrt{5}}}\right)>1$$

加以簡化（上式左邊卽 $\xi_2-\xi_1$），卽得

$$\tau^2<\frac{4}{5}+\delta^2. \tag{12}$$

因在化簡過程中，不等式兩邊皆爲正數，故吾人已經證明：若 (11) 及 (12) 成立，卽 $2\sqrt{\frac{\delta}{\sqrt{5}}}\leqslant\tau<\sqrt{\frac{4}{5}+\delta^2}$，則定理已經成立.

現留待考慮者爲 $\tau^2<\frac{4\delta}{\sqrt{5}}$ 及 $\sqrt{\frac{4}{5}+\delta^2}\leqslant\tau<1$ 兩種情形.

2) 設 $\tau^2<\frac{4\delta}{\sqrt{5}}$. 因 $\tau>0$, 故

$$\xi=\frac{1}{\sqrt{\delta}}\left(\frac{\tau}{2\sqrt{\delta}}+\sqrt{\frac{\tau^2}{4\delta}+\frac{1}{\sqrt{5}}}\right)>\frac{1}{\sqrt{\delta}}\sqrt{\frac{1}{\sqrt{5}}}>1.$$

任與一 $\eta>0$, 取 $\xi_1=\eta$, $\xi_2=\eta+\xi$, 顯然有 $\xi_2-\xi_1=\xi>1$. 故 (9) 中之 x 存在，由假定可知

$$\frac{x}{q}\left(\frac{x\delta}{q}-\tau\right)=\left(\frac{x\sqrt{\delta}}{q}-\frac{\tau}{2\sqrt{\delta}}\right)^2-\frac{\tau^2}{4\delta}>-\frac{1}{\sqrt{5}}.$$

另一方面，命 $y=ax+b$, 則當 x 在一區間內變化時，y^2 在兩端點之一取其極大值，故

$$\frac{x}{q}\left(\frac{x\delta}{q}-\tau\right)=\left(\frac{x\sqrt{\delta}}{q}-\frac{\tau}{2\sqrt{\delta}}\right)^2-\frac{\tau^2}{4\delta}\leqslant$$

$$\leqslant\max\left\{\left(\eta\sqrt{\delta}-\frac{\tau}{2\sqrt{\delta}}\right)^2-\frac{\tau^2}{4\delta},\left((\eta+\xi)\sqrt{\delta}-\frac{\tau}{2\sqrt{\delta}}\right)^2-\frac{\tau^2}{4\delta}\right\}=$$

$$=\max\left\{\eta^2\delta-\eta\tau,\left(\sqrt{\frac{\tau^2}{4\delta}+\frac{1}{\sqrt{5}}}+\eta\sqrt{\delta}\right)^2-\frac{\tau^2}{4\delta}\right\}=$$

$$=\frac{1}{\sqrt{5}}+O(\eta).$$

因 η 可以任意小，故此時定理已經成立.

3) 設 $\sqrt{\frac{4}{5}+\delta^2}\leqslant\tau<1$, 因 $\delta<\frac{1}{\sqrt{5}}$，故

$$\tau\geqslant\sqrt{\frac{4}{5}+\delta^2}>\sqrt{\left(1-\frac{1}{\sqrt{5}}\right)^2+2\delta\left(1-\frac{1}{\sqrt{5}}\right)+\delta^2}=$$

$$=1-\frac{1}{\sqrt{5}}+\delta.$$

即

$$1-\tau<\frac{1}{\sqrt{5}}-\delta.$$

對任一 $\eta>0$, 可以決定整數對 x, y, 使

$$px-qy=[q\beta]+1, \qquad \eta q\leqslant x<(1+\eta)q,$$

則如 (10), 我們有

$$|x\vartheta-y-\beta|=\left|\frac{x\delta}{q^2}+\frac{1-\tau}{q}\right|=\frac{1}{q}\left(\frac{x\delta}{q}+(1-\tau)\right)<$$

$$<\frac{1}{q}\left\{(1+\eta)\delta+\frac{1}{\sqrt{5}}-\delta\right\}\leqslant\frac{1}{q}(1+\eta)\frac{1}{\sqrt{5}}<\frac{(1+\eta)^2}{x\sqrt{5}}.$$

因 η 可以任意小,故定理已完全證明.

習題. 試證明, 若 ϑ 爲一無理數,其對任一 $\varepsilon>0$ 常有整數 x 及 y, 使

$$|x\vartheta-y|<\frac{\varepsilon}{x}.$$

則對任一 $\delta>0$ 及任一實數 β, 常有整數 $x>0$ 及 y, 使

$$|x\vartheta-y-\beta|<\frac{1+\delta}{3x}.$$

§11. 一致分佈及 $n\vartheta$ (mod 1) 之一致分佈性.

上節中之 Чебышев 定理說明了 (0,1) 之間的每一點皆爲點集

$$\{x\vartheta\}=x\vartheta-[x\vartheta] \qquad x=1,2,3,\cdots \tag{1}$$

之一極限點. 但此點集在 (0,1) 間之分佈狀況如何,是否爲一致分佈,換言之,若 (a, b) 爲屬於 (0,1) 中之小區間, 則當 $x=1,2,\cdots,n$ 時, (a, b) 中是否包含此 n 點中其應得之一份,此定理並未給與任何回答. 本節之目的,即在答覆此項問題,我們先將應得之一份予以確切的定義.

定義. 若 $P_i(i=1,2,3,\cdots)$ 爲 (0,1) 中之一點集, 若對任一自然數 n 及任二正數 a, b, $0\leqslant a<b\leqslant 1$, $P_1,\cdots,P_n$, n 個點中,其落入區間 (a, b) 中者的數目 $N_n(a, b)$ 常滿足關係

$$\lim_{n\to\infty}\frac{N_n(a,b)}{n}=b-a,$$

則稱點集 $P_i (i = 1, 2, 3, \cdots)$ 在 (0,1) 內一致分佈.

我們現來證明下之定理:

定理. 若 ϑ 爲一無理數,則點集

$$\{x\vartheta\} = x\vartheta - [x\vartheta] \qquad x = 1, 2, 3, \cdots$$

在 (0,1) 中一致分佈.

證: 設 (a, b) 爲 (0,1) 內之任一小區間. 由定理 4.1 我們有無窮對整數 $q > 0$, p 使

$$\vartheta = \frac{p}{q} + \frac{\delta}{q^2}, \qquad |\delta| < 1, \qquad (p, q) = 1.$$

命 u, v 爲二整數,使

$$\frac{u-1}{q} < a \leqslant \frac{u}{q} < \frac{v}{q} \leqslant b < \frac{v+1}{q},$$

又設 $n = r\, q + s$, $0 \leqslant s < q$, j 爲一整數. $0 \leqslant j < r$, 我們現來看一完全系 (mod q) jq, $jq+1, \cdots, jq+q-1$. 顯而易見,

$$\{(jq+k)\vartheta\} = \left\{\frac{kp}{q} + \frac{j\delta}{q} + \frac{k\delta}{q^2}\right\} = \left\{\frac{kp+[j\delta]}{q} + \frac{\delta'}{q}\right\},$$

$$|\delta'| < 2.$$

因 $[j\delta]$ 與 k 無關,故當 $k = 0, 1, \cdots, q-1$ 時, $pk + [j\delta]$ 亦跑過一完全剩餘系 (mod q), 故 q 個數 $\{(jq+k)\vartheta\}$ 中,其落入 (a, b) 中者多於 $v-u-4$ 個而少於 $v-u+6$ 個, 因之, $\{x\vartheta\}$ $(x = 1, 2, \cdots, n)$ 中, 其落入 (a, b) 中者,多於

$$r(v-u-4) = \frac{n}{q}(v-u-4) - \frac{s}{q}(v-u-4) \geqslant$$

$$\geqslant n(b-a) - \frac{6}{q}n - \frac{v-u-4}{n}n$$

個,而少於

$$(r+1)(v-u+6) \leqslant n\left(\frac{v-u}{q} + \frac{6}{q}\right) + v - u + 6 \leqslant n(b-a) +$$

$$+ \frac{6}{q}n + \frac{v-u+6}{n}n$$

個. 設 $\varepsilon > 0$ 爲任意給定之數,取 q 甚大,使 $\frac{6}{q} < \frac{\varepsilon}{2}$,再取 n 使 $\frac{q+6}{n} < \frac{\varepsilon}{2}$,

則得

$$n(b-a)-n\varepsilon \leqslant N_n(a,b) \leqslant n(b-a)+n\varepsilon.$$

卽

$$\lim_{n\to\infty} \frac{N_n(a,b)}{n} = b-a.$$

§ 12. 一致分佈之判斷條件.

定理 1. 一貫數

$$x_1, \cdots, x_m, \cdots \qquad 0 \leqslant x_m \leqslant 1 \tag{1}$$

是一致分佈之必要且充分條件爲對任一 (0,1) 間 Riemann 可積函數 $f(x)$ 常有

$$\lim_{n\to\infty} \frac{f(x_1)+\cdots+f(x_n)}{n} = \int_0^1 f(x)\,dx. \tag{2}$$

證: 先證明若 (1) 是一致分佈，則 (2) 式成立。

1) 命

$$f(x) = \begin{cases} c, & \text{若 } a \leqslant x \leqslant b, \\ 0, & \text{不在此隔間內}. \end{cases}$$

如此則

$$\lim_{n\to\infty} \frac{f(x_1)+\cdots+f(x_n)}{n} = c \lim_{n\to\infty} \frac{N_n(a,b)}{n} = c(b-a).$$

而另一方面

$$\int_0^1 f(x)\,dx = c(b-a),$$

故定理對此函數爲眞實.

2) (2) 式是一線性關係，卽若對 $f_1, \cdots, f_k$ 能成立，則對線性關聯 $c_1 f_1 + \cdots + c_k f_k$ 亦成立，由 1) 可知當 f 爲階梯函數時也眞實.

3) 習知: 若 f 是一 Riemann 可積函數，則任與 $\varepsilon > 0$ 能有二階梯函數 $\varphi_\varepsilon(x)$, $\Phi_\varepsilon(x)$ 使

$$\varphi_\varepsilon(x) \leqslant f(x) \leqslant \Phi_\varepsilon(x), \qquad 0 \leqslant x \leqslant 1. \tag{3}$$

且使

$$\int_0^1 (\Phi_\varepsilon(t) - \varphi_\varepsilon(t))\,dt < \varepsilon. \tag{4}$$

由 2) 已知本定理對 $\Phi_\varepsilon(x)$ 及 $\varphi_\varepsilon(x)$ 眞實，故

$$\int_0^1 \varphi_\varepsilon(t)\,dt = \lim_{n\to\infty} \frac{1}{n}(\varphi_\varepsilon(x_1)+\cdots+\varphi_\varepsilon(x_n)) \leqslant$$

$$\leqslant \lim_{n\to\infty} \frac{1}{n}(f(x_1)+\cdots+f(x_n)) \leqslant$$

$$\leqslant \lim_{n\to\infty} \frac{1}{n}(\Phi_\varepsilon(x_1)+\cdots+\Phi_\varepsilon(x_n)) = \int_0^1 \Phi_\varepsilon(t)\,dt.$$

又由 (3) 可知

$$\int_0^1 \varphi_\varepsilon(t)\,dt \leqslant \int_0^1 f(x)\,dx \leqslant \int_0^1 \Phi_\varepsilon(x)\,dx.$$

故得

$$\left| \lim_{n\to\infty} \frac{f(x_1)+\cdots+f(x_n)}{n} - \int_0^1 f(x)\,dx \right| < \varepsilon.$$

此證明了本定理之必要部分.

定理之充分部分極易證明：僅取

$$f(x) = \begin{cases} 1, & 若\ a \leqslant x \leqslant b, \\ 0, & 若不然. \end{cases}$$

(2) 式卽變爲

$$\lim_{n\to\infty} \frac{N_n(a,b)}{n} = b - a.$$

附註： 在應用時本定理十分困難,蓋須要對所有的 Riemann 可積函數進行研究才能證明一致分佈性也. 但以上證明中指出一點： 用所有的階梯函數卽已足够,實際上說明： 如一函數組能够以其線性式接近所有的 Riemann 可積函數,卽合所求. 此乃以下定理之所由來.

定理 2. 在定理 1 之假定下,另一必要且充分之條件爲 (2) 式對 $f(x) = e^{2\pi imx}$ $(m = \pm 1, \pm 2, \cdots)$ 眞實.

換言之,貫 (1) 爲一致分佈之必要且充分之條件爲對任一整數 $m \neq 0$, 常有

$$\lim_{n\to\infty} \frac{1}{n} \left| \sum_{\nu=1}^{n} e^{2\pi imx_\nu} \right| = 0.$$

證： 必要性毋待證明,今往證其充分性,定義

$$g(x) = \begin{cases} 1, & 若\ 0 \leqslant x < a, \\ 0, & 若\ a \leqslant x < 1. \end{cases}$$

則

$$\lim_{n\to\infty}\frac{g(x_1)+\cdots+g(x_n)}{n}=\lim_{n\to\infty}\frac{N_n(0,a)}{n}.$$

故若能證明

$$\lim_{n\to\infty}\frac{g(x_1)+\cdots+g(x_n)}{n}=a,$$

則定理已明. 今往做出以 1 爲周期之一連續函數 $g_{\eta,\delta}(x)$ 來接近 $g(x)$. 定義

$$g_{\eta,\delta}(x)=\begin{cases}(x-\eta+\delta)/\delta, & 若\ \eta-\delta\leqslant x\leqslant\eta,\\ 1, & 若\ \eta\leqslant x\leqslant a-\eta,\\ -(x-a+\eta-\delta)/\delta, & 若\ a-\eta\leqslant x\leqslant a-\eta+\delta,\\ 0, & 若\ a-\eta+\delta\leqslant x\leqslant\eta-\delta+1.\end{cases}$$

此處 $0<\delta\leqslant\frac{1}{2}\min(a,1-a)$, $0\leqslant\eta\leqslant\delta$. 顯然

$$g_{\delta,\delta}(x)\leqslant g(x)\leqslant g_{0,\delta}(x).$$

由於 $g_{\eta,\delta}(x)$ 是一連續函數,故

$$g_{\eta,\delta}(x)=\sum_{n=-\infty}^{\infty}C_n e^{2\pi inx},$$

此處

$$C_0=\int_{\eta-\delta}^{\eta-\delta+1}g_{\eta,\delta}(x)\,dx=a+\delta-2\eta;$$

且當 $n\neq0$,

$$C_n=\int_{\eta-\delta}^{\eta-\delta+1}e^{-2\pi inx}g_{\eta,\delta}(x)\,dx=$$

$$=\frac{e^{-n\pi ia}}{\delta(n\pi)^2}\sin n\pi(a+\delta-2\eta)\sin n\pi\delta.$$

故可見

$$|C_n|\leqslant\frac{1}{\delta(n\pi)^2}.$$

故得

$$S_{\eta,\delta}(x)=\frac{g_{\eta,\delta}(x_1)+\cdots+g_{\eta,\delta}(x_k)}{k}=$$

$$=\frac{1}{k}\sum_{j=1}^{k}\sum_{n=-\infty}^{\infty}C_n e^{2\pi inx_j}=$$

$$= \frac{1}{k} \sum_{n=-\infty}^{\infty} C_n \sum_{j=1}^{k} e^{2\pi i n x_j}.$$

如此則

$$S_{\eta,\delta}(x) = C_0 + \sum_{\substack{n=-N \\ n\neq 0}}^{N} C_n \frac{1}{k} \sum_{j=1}^{k} e^{2\pi i n x_j} +$$

$$+ \sum_{|n|>N} C_n \frac{1}{k} \sum_{j=1}^{k} e^{2\pi i n x_j}.$$

今有

$$\left| \sum_{|n|>N} C_n \frac{1}{k} \sum_{j=1}^{k} e^{2\pi i n x_j} \right| \leqslant \frac{2}{\delta \pi^2} \sum_{n>N} \frac{1}{n^2}.$$

當 N 充分大時,可使此不等式之右邊 $<\varepsilon$. 固定此 N, 由於

$$\lim_{k\to\infty} \frac{1}{k} \sum_{j=1}^{k} e^{2\pi i n x_j} = 0,$$

故可取 k 充分大使

$$\left| \sum_{\substack{n=-N \\ n\neq 0}}^{N} C_n \frac{1}{k} \sum_{j=1}^{k} e^{2\pi i n x_j} \right| < \varepsilon.$$

卽對任一對固定的 η, δ 常有

$$|S_{\eta,\delta}(x) - (a+\delta-2\eta)| < 2\varepsilon,$$

卽

$$\lim_{k\to\infty} S_{\eta,\delta}(x) = a + \delta - 2\eta.$$

命

$$S(x) = \frac{g(x_1) + \cdots + g(x_k)}{k}.$$

由於

$$S_{\delta,\delta}(x) \leqslant S(x) \leqslant S_{0,\delta}(x),$$

故對任一 δ 常有

$$a - \delta \leqslant \varliminf_{k\to\infty} S \leqslant \varlimsup_{k\to\infty} S \leqslant a + \delta.$$

卽得

$$\lim_{k\to\infty} S = a.$$

此證明了本定理.

附記：爲了更清楚地說明一致分佈性，最好利用單位圓來代表單位區間．命

$$\xi_n = e^{2\pi i x_n}, \qquad n = 1, 2, \cdots,$$

如此則將貫 (1) 變爲單位圓周上之一貫．此種表法優點之一是在將區間 (0,1) 之二端點 0,1 之特殊性予以銷除．在圓上任取一弧段，其長爲 $2\pi\alpha$, $(\alpha < 1)$, 則一致分佈之點貫落在此弧中之個數佔全點貫之 α 倍．由於對任一整數 d 常有

$$e^{2\pi i x_n} = e^{2\pi i (x_n + d)},$$

故可以不一定假定貫 (1) 在 (0,1) 之中．即可以定義：若一函數 $f(x)$ 之分數部份在 (0,1) 中一致分佈，則謂 $f(x)$ 一致分佈，mod 1．而其必要且充分條件爲：對任一整數 $m(\neq 0)$，有

$$\lim_{n\to\infty} \frac{1}{n} \sum_{x=1}^{n} e^{2\pi i m f(x)} = 0 .$$

此式之意義謂：對任一 $m \neq 0$，點列

$$e^{2\pi i m f(x)}, \qquad x = 1, 2, \cdots$$

之重心爲圓心．顯然可見，如果 $f(x)$ 一致分佈，mod 1，則對任一非零之整數 m，$mf(x)$ 也一致分佈，mod 1．

在一致分佈問題之研究中，最有趣而尙未解決之問題爲 e^x 是否一致分佈，mod 1．

定理 3. 函數 $f(x)$ 爲一致分佈，mod 1 的充分且必要之條件爲對任何 $0 \leqslant a \leqslant 1$，皆有

$$\lim_{n\to\infty} \frac{1}{n} \sum_{x=1}^{n} \{f(x)+a\} = \frac{1}{2}.$$

證： 必要性：若 $f(x)$ 爲一致分佈，mod 1，則 $f(x)+a$ 亦爲一致分佈，mod 1．故只須就 $a=0$ 來證明條件爲必要卽可．令 $x_m = \{f(m)\}$，則因定理 1 卽得

$$\lim_{n\to\infty} \frac{1}{n} \sum_{x=1}^{n} \{f(x)\} = \int_0^1 x\,dx = \frac{1}{2}.$$

充分性：設 $0 \leqslant b \leqslant 1$，則

$$\frac{1}{n} \sum_{x=1}^{n} \{f(x)+1-b\} = \frac{1}{n} \sum\nolimits_1 (\{f(x)\}+1-b) +$$

$$+\frac{1}{n}\sum\nolimits_2(\{f(x)\}-b),$$

此處 $\sum_1$ 中之 x 跑過 $1,2,\cdots,n$ 中使 $\{f(x)\}<b$ 的各數，$\sum_2$ 中之 x 則跑過 $1,2,\cdots,n$ 中使 $\{f(x)\}\geqslant b$ 的各數，由是卽得

$$\frac{1}{n}\sum_{x=1}^{n}\{f(x)+1-b\}=n^{-1}\sum_{x=1}^{n}\{f(x)\}+n^{-1}N_n(0,b)-b.$$

命 $n\to\infty$ 並注意定理之假定，卽得

$$\lim_{n\to\infty}\frac{1}{n}N_n(0,b)=b.$$

明所欲證。

第十一章
不定方程

§1. 引言. 所謂不定方程乃指變數之數多於方程之個數,且未知數須受某種限制(如整數,正整數或有理數等)之方程而言. 舍一次,二次外,不定方程之討論,異常瑣碎. Dickson 於其所著之數論史之第二册中專論此項方程,共佔八百餘頁,其繁碎性及複雜性,概可想見. 此類方程肇源頗古,三世紀初有 Diophantus 者,曾建議若干此類問題. 故今仍有沿用 Diophantus 氏方程之名者. 我國周髀算經之商高定理

"句三股四而弦五"

亦爲此類問題之濫觴,考其時期遠在Diophantus之前. 由商高定理立卽聯想到:求直角三角形之各邊皆爲整數者,換言之,求整數 x, y, z 使

$$x^2+y^2=z^2.$$

此將於 §6 中解決之.

§2. 一次不定方程. 由定理 2.6.2 已知不定方程

$$a_1x_1+a_2x_2+\cdots+a_nx_n=N$$

可解之必要且充分之條件爲

$$(a_1,\cdots,a_n)\mid N.$$

今設 $a_1>0,\ a_2>0,\ \cdots,\ a_n>0,\ (a_1,\cdots,a_n)=1$, 問當 $N\to\infty$ 時,

$$a_1x_1+a_2x_2+\cdots+a_nx_n=N,\qquad x_\nu\geqslant 0\qquad (\nu=1,2,\cdots,n)\tag{1}$$

之解答數之無窮大之階若何?(未讀微積分之讀者可以略去本節之其餘部分.)

定理 1. 設 $(a_1,\cdots,a_n)=1$. 命 $A(N)$ 表 (1) 式之解數,則

$$\lim_{N\to\infty}\frac{A(N)}{N^{n-1}}=\frac{1}{a_1a_2\cdots a_n(n-1)!}.$$

證: 1) 因 $(a_1,\cdots,a_n)=1$, 故 $A(N)$ 爲

$$f(x) = \frac{1}{1-x^{a_1}} \cdot \frac{1}{1-x^{a_2}} \cdot \cdots \cdot \frac{1}{1-x^{a_n}}$$

之 x^N 之係數. 命

$$1, \zeta_1, \zeta_2, \cdots, \zeta_t$$

爲 $(1-x^{a_1})(1-x^{a_2})\cdots(1-x^{a_n})=0$ 之諸根. 其重數各爲

$$n, l_1, \cdots, l_t.$$

因 $(a_1, a_2, \cdots, a_n)=1$, 故 $l_i \leqslant n-1$ $(i=1, 2, \cdots, t)$.

用部分分式法得

$$\begin{aligned} f(x) = \frac{A_n}{(1-x)^n} + \cdots + \frac{A_1}{1-x} + \\ + \frac{B_{l_1}}{(\zeta_1-x)^{l_1}} + \cdots + \frac{B_1}{\zeta_1-x} + \\ + \cdots\cdots\cdots + \\ + \frac{P_{l_t}}{(\zeta_t-x)^{l_t}} + \cdots + \frac{P_1}{\zeta_t-x}, \end{aligned} \tag{2}$$

此處 $A, B, \cdots, P$ 皆爲常數.

2) 命

$$\frac{A}{(\alpha-x)^l} = A\alpha^{-l}\left(1-\frac{x}{\alpha}\right)^{-l}$$

之展開式中 x^N 之係數爲 $\psi(N)$, 則由二項式展開定理,可得

$$\begin{aligned} \psi(N) &= A\,\alpha^{-l}\frac{(-l)(-l-1)\cdots(-l-N+1)}{N!}\left(-\frac{1}{\alpha}\right)^N = \\ &= A\,\alpha^{-l}\frac{(N+l-1)(N+l-2)\cdots(N+1)}{(l-1)!}\left(\frac{1}{\alpha}\right)^N. \end{aligned}$$

於是

$$\lim_{N\to\infty}\frac{\psi(N)\cdot\alpha^{l+N}}{N^{l-1}} = \frac{A}{(l-1)!}. \tag{3}$$

依法展開 (2) 式中之各項,其 x^N 之係數 $A(N)$ 必適合

$$\lim_{N\to\infty}\frac{A(N)}{N^{n-1}} = \frac{A_n}{(n-1)!},$$

因 $l_i \leqslant n-1$ 故也.

3) 由 (2) 可得

$$A_n = \lim_{x\to 1} \frac{(1-x)^n}{(1-x^{a_1})\cdots(1-x^{a_n})} =$$

$$= \frac{1}{a_1\cdots a_n}.$$

定理 2. 當 N 充分大時，(1) 式必可解. 所謂充分大云者，乃謂有一正數 C 存在，凡大於 C 之整數 N，(1) 式常有解答之意.

習題. 若 $(a, b)=1$, $a>0$, $b>0$, 則

$$ax+by=N, \quad x\geqslant 0, \quad y\geqslant 0$$

之解數爲

$$\frac{N-(bl+am)}{ab}+1,$$

此處之 l 爲 $bl\equiv N \pmod a$ 之最小非負解答，又 m 爲 $am\equiv N \pmod b$ 之最小非負解答.

§ 3. 二次不定方程.

今往解不定方程

$$ax^2+bxy+cy^2+dx+ey+f=0. \tag{1}$$

命 $D=b^2-4ac$. 若 $D=0$, 則以 $4a$ 乘 (1) 式得

$$(2ax+by)^2+4adx+4aey+4af=0.$$

此類不定方程之解法不難. 命 $2ax+by=t$, 則

$$t^2+2(2ae-bd)y+4af=-2dt,$$

$$(t+d)^2=2(bd-2ae)y+d^2-4af.$$

先由同餘式

$$(t+d)^2\equiv d^2-4af \quad (\mathrm{mod}\ 2(bd-2ae))$$

求 t，再由是求出 y 及 x.

今設 $D\neq 0$. 以 D^2 乘 (1) 式，則

$$aD^2x^2+bD^2xy+cD^2y^2+dD^2x+eD^2y+fD^2=0. \tag{2}$$

命

$$Dx=x'+2cd-be, \quad Dy=y'+2ae-bd.$$

代入 (2) 式

$$a(x'+2cd-be)^2+b(x'+2cd-be)(y'+2ae-bd)+c(y'+2ae-bd)^2+$$

$$+ dD(x' + 2cd - be) + eD(y' + 2ae - bd) + fD^2 = 0,$$

卽

$$ax'^2 + bx'y' + cy'^2 = k, \tag{3}$$

此處

$$-k = a(2cd - be)^2 + b(2cd - be)(2ae - bd) + c(2ae - bd)^2 +$$
$$+ dD(2cd - be) + eD(2ae - bd) + fD^2.$$

故 (1) 式是否可解,實依賴於 (3) 式能否有適合

$$x' \equiv be - 2cd, \quad y' \equiv bd - 2ae \pmod D$$

之解答. 故解不定方程 (3) 乃一先決問題.

§ 4. 解 $ax^2 + bxy + cy^2 = k$.

今往解

$$ax^2 + bxy + cy^2 = k. \tag{1}$$

命 $d = b^2 - 4ac$. 今假定 d 非平方數及 $(a, b, c) = 1$. 且祇須求解之適合 $(x, y) = 1$ 者, 如此之解謂之旣約解 (proper solution).

定理 1. 若 x, y 爲一旣約解,則可唯一定出二整數 s 及 r 使

$$xs - yr = 1 \tag{2}$$

及

$$l = (2ax + by) r + (bx + 2cy) s$$

適合

$$l^2 \equiv d \pmod{4k}, \quad 0 \leqslant l < 2k. \tag{3}$$

證: 命 r_0, s_0 爲 (2) 之一解,則 (2) 之諸解爲

$$r = r_0 + hx, \quad s = s_0 + hy,$$

此處 h 爲一任意之整數. 由是

$$l = (2ax + by) r_0 + (bx + 2cy) s_0 + 2h(ax^2 + bxy + cy^2) =$$
$$= l_0 + 2hk.$$

故可唯一的 h 使 $0 \leqslant l < 2k$. 又

$$l^2 = [(2ax + by) r + (bx + 2cy) s]^2 =$$
$$= 4(ar^2 + brs + cs^2)(ax^2 + bxy + cy^2) + (b^2 - 4ac)(xs - yr)^2 \equiv$$
$$\equiv d \pmod{4k}.$$

定理 2. 若 (x_1, y_1) 與 (x_2, y_2) 爲對應於同一 l 之二既約解，則其間有次之關係

$$2ax_1 + (b + \sqrt{d})\, y_1 = (2ax_2 + (b + \sqrt{d})\, y_2)\left(\frac{t+u\sqrt{d}}{2}\right), \tag{4}$$

此處之 t 及 u 爲

$$t^2 - du^2 = 4 \tag{5}$$

之整數解. 反之，若 x_2, y_2 是一既約解，則由 (4) 所定義之 x_1, y_1 亦爲一既約解，且有相同之 l.

證： 1） 今先往證明

$$\left.\begin{aligned} t &= ((2ax_1 + by_1)(2ax_2 + by_2) - dy_1 y_2) / 2ak \\ u &= -(x_1 y_2 - x_2 y_1) / k \end{aligned}\right\} \tag{6}$$

卽合所求. 今所需證者爲 t 及 u 均爲整數，且適合 (5) 式. 因

$$\frac{t \mp u\sqrt{d}}{2} = \frac{(2ax_1+by_1)(2ax_2+by_2)-dy_1 y_2 \pm 2a(x_1 y_2 - x_2 y_1)\sqrt{d}}{4ak} =$$

$$= \frac{(2ax_1+by_1 \mp \sqrt{d}\, y_1)(2ax_2+by_2 \pm \sqrt{d}\, y_2)}{(2ax_1+by_1+\sqrt{d}\, y_1)(2ax_1+by_1-\sqrt{d}\, y_1)} =$$

$$= \frac{(2ax_1+by_1 \mp \sqrt{d}\, y_1)(2ax_2+by_2 \pm \sqrt{d}\, y_2)}{(2ax_2+by_2+\sqrt{d}\, y_2)(2ax_2+by_2-\sqrt{d}\, y_2)},$$

故 (4) 式成立. 又因

$$\frac{t^2-du^2}{4} = \frac{t+\sqrt{d}\,u}{2} \cdot \frac{t-\sqrt{d}\,u}{2} = 1,$$

卽 t 及 u 適合 (5) 式. 又

$$\begin{aligned} 2ax_1 + by_1 &= (2ax_1 + by_1)(s_1 x_1 - r_1 y_1) = \\ &= (2ax_1 + by_1) s_1 x_1 - ly_1 + (bx_1 + 2cy_1) s_1 y_1 \equiv \\ &\equiv -ly_1 \pmod{2k}. \end{aligned} \tag{7}$$

同法

$$2ax_2 + by_2 \equiv -ly_2 \pmod{2k}.$$

故

$$2a(x_1 y_2 - x_2 y_1) \equiv 0 \pmod{2k},$$

$$(b + l)(x_1 y_2 - x_2 y_1) \equiv 0 \pmod{2k}.$$

同法

$$2c(x_1 y_2 - x_2 y_1) \equiv 0 \pmod{2k},$$
$$(b-l)(x_1 y_2 - x_2 y_1) \equiv 0 \pmod{2k}.$$

但

$$(2a, b+l, b-l, 2c) = (2a, 2b, 2c, b+l) \leqslant 2,$$

故

$$x_1 y_2 - x_2 y_1 \equiv 0 \pmod{k}.$$

即 u 爲整數. 故 t^2 亦爲整數. 但已知 t 爲有理數,故 t 亦爲整數.

2) 設

$$2ax_1 + (b+\sqrt{d})\,y_1 = (2ax_2 + (b+\sqrt{d})\,y_2)\left(\frac{t+u\sqrt{d}}{2}\right),$$

且 $t^2 - du^2 = 4$, 則

$$x_1 = \frac{t-bu}{2}x_2 - cuy_2, \qquad y_1 = aux_2 + \frac{t+bu}{2}y_2.$$

設 r_1, s_1 對應於解 x_1, y_1, 則

$$r_2 = \frac{t+bu}{2}r_1 + cus_1, \qquad s_2 = -aur_1 + \frac{t-bu}{2}s_1$$

對應於解 x_2, y_2. 蓋

$$1 = x_1 s_1 - y_1 r_1 = \left(\frac{t-bu}{2}x_2 - cuy_2\right)s_1 - \left(aux_2 + \frac{t+bu}{2}y_2\right)r_1 =$$
$$= x_2\left(\frac{t-bu}{2}s_1 - aur_1\right) - y_2\left(cus_1 + \frac{t+bu}{2}r_1\right) =$$
$$= x_2 s_2 - y_2 r_2.$$

又命 l_1, l_2 各對應於 (x_1, y_1) 及 (x_2, y_2). 則

$$l_1 = 2ax_1 r_1 + b(x_1 s_1 + y_1 r_1) + 2cy_1 s_1 =$$
$$= (2ar_1 + bs_1)\left(\frac{t-bu}{2}x_2 - cuy_2\right) + (br_1 + 2cs_1)\left(aux_2 + \frac{t+bu}{2}y_2\right) =$$
$$= \left\{2a\left(r_1\frac{t-bu}{2} + s_1 cu\right) + b\left(s_1\frac{t-bu}{2} + r_1 au\right)\right\}x_2 +$$
$$+ \left\{b\left(r_1\frac{t+bu}{2} - s_1 cu\right) + 2c\left(s_1\frac{t+bu}{2} - r_1 au\right)\right\}y_2 =$$
$$= 2ax_2 r_2 + b(x_2 s_2 + y_2 r_2) + 2cy_2 s_2 = l_2.$$

故得所言.

今分 $d>0$ 及 $d<0$ 兩種情形論之.

定理 3. 設 $d<0$. 命

$$w=\begin{cases}2 & 若\ d<-4,\\ 4 & 若\ d=-4,\\ 6 & 若\ d=-3.\end{cases}$$

則 (1) 式有 w 個既約解對應於同一 l.

證: 由定理 2, 我們祇須證明對應於所與之 d, 方程

$$t^2-du^2=4$$

之解數爲 w 卽可.

若 $d<-4$, 顯然祇有 $t=\pm 2$, $u=0$ 二解. 故 $w=2$.

若 $d=-4$, 則

$$t^2+4u^2=4,$$

此式祇有 $t=\pm 2$, $u=0$ 及 $t=0$, $u=\pm 1$ 四解.

若 $d=-3$, 則

$$t^2+3u^2=4.$$

此式有且僅有次之六解:

$$t=\pm 1,\quad u=\pm 1;\quad t=\pm 2,\quad u=0.$$

定理 4. 若 $d>0$, 則

$$x^2-dy^2=4$$

之諸解,可由次法得之:

命 x_0, y_0 爲上式之解中使 $x_0+y_0\sqrt{d}$ 最小者 ($x_0>0$, $y_0>0$). 則此式之所有的解 x, y 可由

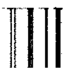
$$\frac{x+y\sqrt{d}}{2}=\pm\left(\frac{x_0+y_0\sqrt{d}}{2}\right)^n,\qquad n\gtreqless 0$$

得出之.

此定理之證明與定理 10.9.2 同, 蓋已知此式必有解答也 (因 $x^2-dy^2=1$ 必有解).

命

$$\varepsilon=\frac{x_0+y_0\sqrt{d}}{2},\qquad \bar{\varepsilon}=\frac{x_0-y_0\sqrt{d}}{2}.$$



定 義. 設 $d>0$, (1) 式之解之適合

$$2ax+(b-\sqrt{d})y>0, \qquad 1\leqslant\left|\frac{2ax+(b+\sqrt{d})y}{2ax+(b-\sqrt{d})y}\right|<\varepsilon^2$$

者名為原解 (primary solution).

若書

$$L=2ax+(b+\sqrt{d})y, \qquad \bar{L}=2ax+(b-\sqrt{d})y,$$

則上之條件變為

$$\bar{L}>0, \qquad 1\leqslant\left|\frac{L}{\bar{L}}\right|<\varepsilon^2.$$

定 理 5. 若 $d>0$,對應於同一 l,(1)式如有既約原解,則只有唯一既約原解.

證: 由定理 2 已知,若 x_0, y_0 為 (1) 式之一既約原解,命 L_0 為其對應之 L, 則凡 (1) 式中對應於同一 l 之既約解皆可表為

$$L=\pm L_0\varepsilon^n$$

之形; 已知

$$\left|\frac{L}{\bar{L}}\right|=\left|\frac{L_0\varepsilon^n}{\bar{L}_0\bar{\varepsilon}^n}\right|=\left|\frac{L_0}{\bar{L}_0}\right|\varepsilon^{2n}.$$

只有當 $n=0$ 時有

$$1\leqslant\left|\frac{L}{\bar{L}}\right|<\varepsilon^2.$$

此時

$$\bar{L}=\bar{L}_0>0.$$

故得定理.

若 $d>0$, 命 $w=1$.

今推廣原解之定義: 當 $d>0$ 時,原解定義如前;而若 $d<0$, 則凡既約解皆名為原解. 於是定理 3 及 5 可合併為:

定 理 6. 對應於同一 l, (1) 式如有既約原解,則只有 w 個既約原解.

定理 5 建議吾人求

$$ax^2+bxy+cy^2=k$$

之解時,不必在整個的雙曲線上摸索. 原解僅在一有限的雙曲線上. 獲得原解後,可由公式 $L=\pm L_0\varepsilon^n$ 以求出所有的解. 卽若 ε 已知, 僅須經有限手續卽可獲得所有的解. 切實言之,從

$$L_0\bar{L}_0=4ak, \quad \bar{L}_0>0, \quad 1\leqslant\left|\frac{L_0}{\bar{L}_0}\right|<\varepsilon^2,$$

可知

$$|\bar{L}_0| \leqslant |L_0| = \sqrt{\left|\frac{L_0\bar{L}_0}{\bar{L}_0}\right|^2} = 2\sqrt{|ak|}\sqrt{\left|\frac{L_0}{\bar{L}_0}\right|} < 2\sqrt{|ak|}\,\varepsilon,$$

即

$$|2\sqrt{d}\ y| = |L_0 - \bar{L}_0| \leqslant |L_0| + |\bar{L}_0| <$$
$$< 4\sqrt{|ak|}\,\varepsilon,$$

即

$$|y| \leqslant 2\varepsilon\sqrt{|ak|/d}.$$

僅須尋求適合 $0 < y \leqslant 2\varepsilon\sqrt{|ak|/d}$ 之解,其餘可由公式 $L = \pm L_0\varepsilon^n$ 得之.

當 $a > 0$, $k > 0$ 時,由 $\bar{L} > 0$ 及 $L\bar{L} > 0$, 可知 $L > 0$. 因之, 結合 $\bar{L} < L$, 可得

$$0 < 2\sqrt{d}\ y = L - \bar{L} \leqslant L = \sqrt{L\bar{L}\frac{L}{\bar{L}}} \leqslant$$
$$\leqslant \varepsilon\sqrt{4ak}.$$

故得

$$0 < y \leqslant \varepsilon\sqrt{ak/d}.$$

此結果在實際計算時,略佳於以前所給之限.

習題 1. 如上述之假定,證明

$$0 < y \leqslant \left(\varepsilon - \frac{1}{\varepsilon}\right)\sqrt{ak/d}.$$

習題 2. 證明

$$x_1 = \frac{t-bu}{2}x - cuy, \qquad y_1 = aux + \frac{t+bu}{2}y$$

變 $ax^2 + bxy + cy^2$ 爲 $ax_1^2 + bx_1y_1 + cy_1^2$.

§5. 求解方法.

由前已知,吾人須求出

$$ax^2 + bxy + cy^2 = k$$

之諸解. 今就 $d > 0$ 且非平方數之情況討論之. 此式可寫爲

$$(2ax + by)^2 - dy^2 = 4ak.$$

故解次之二次式

$$x^2 - dy^2 = \delta k, \quad k > 0, \quad \delta = \pm 1 \tag{1}$$

乃第一要事. 若 $k < \sqrt{d}$, 則由定理 10. 8. 3 可知:所有 (1) 之解可從 $\sqrt{d}$ 之漸近分數中逐一試出 (因週期性, 故此項手續有限).

今再說明,若 $k > \sqrt{d}$, 則亦可以化成 $k < \sqrt{d}$ 之情形討論之.

設 x, y 爲 (1) 之既約解. 則有 x_1 及 y_1 使

$$xy_1 - yx_1 = \delta. \tag{2}$$

以 $x_1^2 - dy_1^2$ 乘 (1) 式之兩邊. 可得

$$(xx_1 - dyy_1)^2 - d(xy_1 - x_1y)^2 = \delta k(x_1^2 - dy_1^2),$$

即

$$(xx_1 - dyy_1)^2 - d = \delta k(x_1^2 - dy_1^2).$$

命 x_0, y_0 爲 (2) 之一解. 則 (2) 之諸解爲

$$x_1 = x_0 + tx, \quad y_1 = y_0 + ty.$$

故

$$xx_1 - dyy_1 = xx_0 - dyy_0 + (x^2 - dy^2)t =$$
$$= xx_0 - dyy_0 + \delta tk.$$

故可取 t 之值使

$$|xx_1 - dyy_1| \leqslant \frac{k}{2}.$$

命 $|xx_1 - dyy_1| = l$, 即得

$$x_1^2 - dy_1^2 = \frac{l^2 - d}{\delta k} = \eta h, \quad \eta = \pm 1, \quad h > 0.$$

則

$$h \leqslant \frac{\max(d, l^2)}{k} < \frac{k^2}{k} = k.$$

由此可見,由 (1) 式之一解,可以得出一同樣之方程,其 k 較前爲小者. 若仍比 $\sqrt{d}$ 爲大,則可續行此法. 此種討論建議次之方法.

先求諸 l, 使

$$l^2 \equiv d \pmod{k}, \quad 0 \leqslant l \leqslant \frac{k}{2}$$

者, 命之爲

$$l_1, \cdots, l_t.$$

命 $(l_i^2-d)/\delta k=\eta_i h_i$, $\eta_i=\pm 1$, $h_i>0$. 解方程

$$x_1^2-dy_1^2=\eta_1 h_1,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$x_1^2-dy_1^2=\eta_t h_t.$$

假定 $h_i<\sqrt{d}$, 則由連分數的方法解此方程. 命 x_i, y_i 爲其一解. 則

$$x=\frac{-\delta d y_i \pm l_i x_i}{\eta_i h_i}, \qquad y=\frac{-\delta x_i \pm l_i y_i}{\eta_i h_i} \tag{3}$$

爲 (1) 式之解. 蓋由

$$\eta_i h_i(x+\sqrt{d}\,y)=(x_i+\sqrt{d}\,y_i)(-\delta\sqrt{d}\pm l_i)$$

卽得

$$x^2-dy^2=\delta k.$$

又若 (3) 式中的 x, y 爲整數,則此對 x, y 卽爲所求.

若仍有 $h_i>\sqrt{d}$, 則如法進行, 可得

$$x_i^2-dy_i^2=\eta_i h_i$$

之一切解. 因而得到 (1) 之所有解. 今舉一例以明之:

例. 求解

$$x^2-15y^2=61. \tag{4}$$

先求適合

$$l^2\equiv 15 \pmod{61}, \qquad 0\leqslant l\leqslant \frac{61}{2}$$

之諸解. 卽於

$$l^2=15+61h, \qquad l^2\leqslant 900$$

中求 h 使 $15+61h$ 成平方數者. 令 h 經過 $0\leqslant h\leqslant\left[\frac{900}{61}\right]=14$, 逐一代入後,知祇當 $h=10$ 時爲然, 其時

$$l=25, \qquad h=10.$$

故今須求

$$x_1^2-15y_1^2=10 \tag{5}$$

之解. 但 10 仍大於 $\sqrt{15}$, 故再求

$$l^2 = 15 + 10h, \qquad l \leqslant \frac{10}{2} = 5$$

之解. 此祇當 $l=5$, $h=1$ 爲然, 故須求解

$$x_2^2 - 15y_2^2 = 1. \tag{6}$$

由連分數法,知 (6) 之解答爲

$$x_2 + \sqrt{15}\, y_2 = \pm (4 + \sqrt{15})^n.$$

故

$$x_1 + \sqrt{15}\, y_1 = \pm (4 + \sqrt{15})^n (5 \pm \sqrt{15}),$$

而

$$x + \sqrt{15}\, y = \pm (4 + \sqrt{15})^n (5 \pm \sqrt{15})(25 \pm \sqrt{15})/10.$$

此處之三個 $\pm$ 號各不相關. 故得

$$x + \sqrt{15}\, y = \pm (4 + \sqrt{15})^n (14 \pm 3\sqrt{15})$$

$$或 = \pm (4 + \sqrt{15})^n (11 \pm 2\sqrt{15}).$$

另一方法,可由 §4 之末所列之不等式算出之,卽 $0 < y \leqslant \varepsilon\sqrt{ak/d}$. 在本例中得出 $0 < y \leqslant 7$. 作次表

y	1	2	3	4	5	6	7
$15(2y-1)$	15	45	75	105	135	165	195
$15y^2$	15	60	135	240	375	540	735
$15y^2+61$	76	**121**	**196**	301	436	601	796

此表之造法如次: 第一行無待解釋. 第二行中之每一項乃由前一項加 30 而得者. 第三行中之第 i 項乃由第 $i-1$ 項加第二行中第 i 項而得者. 第四行乃由第三行加 61 得之,更毋待言.

習 題 1. 求下列諸不定方程之諸解

(a) $3x^2 - 8xy + 7y^2 - 4x + 2y = 109$,

(b) $3xy + 2y^2 - 4x - 3y = 12$,

(c) $9x^2 - 12xy + 4y^2 + 3x + 2y = 12$,

(d) $x^2 - 8xy - 17y^2 + 72y - 75 = 0$.

習題 2. 設 $k<\sqrt{d}$. 求證

$$ax^2+bxy+cy^2=k$$

之解,可由

$$ax^2+bx+c=0$$

之根之漸近分數得之. 試推廣本節之結果.

§6. 商高定理之推廣.

求

$$x^2+y^2=z^2$$

之諸整數解.

若 $(x, y)=d>1$, 則 d 亦為 z 之因數. 故討論此方程式之解時,可設 $(x, y)=1$. 其他之解悉可由此類之解乘以一數而得之. 又顯然祇須求解之適合 $x>0$, $y>0$ 及 $z>0$ 者.

x 及 y 中必有一為偶數. 不然,則

$$x^2\equiv y^2\equiv 1 \pmod 4,$$

即

$$x^2+y^2\equiv 2 \pmod 4.$$

亦即 z^2 為 2 之倍數,而非 4 之倍數,此不可能. 故可設欲求之解中, x 為偶數.

定理 1. 不定方程

$$x^2+y^2=z^2 \tag{1}$$

之解適合

$$x>0,\quad y>0,\quad z>0,\quad (x, y)=1,\quad 2\mid x \tag{2}$$

者,必可表為

$$x=2ab,\quad y=a^2-b^2,\quad z=a^2+b^2, \tag{3}$$

$$(a, b)=1,\quad a>b>0,\quad a, b \text{ 中一奇一偶}. \tag{4}$$

如此之 (x, y, z) 與 (a, b) 成一一對應,即不同之 (a, b),對應於不同之 (x, y, z),且反之亦然.

證: 1) 由 (1), (2) 以求 (3), (4). 因 y 及 z 皆為奇數,故 $\frac{z-y}{2}$, $\frac{z+y}{2}$ 皆為整數,又

$$\left(\frac{z-y}{2},\ \frac{z+y}{2}\right)=(z,y)=1.$$

由 (1) 立得

$$\left(\frac{x}{2}\right)^2=\frac{z+y}{2}\cdot\frac{z-y}{2},$$

故

$$\frac{z+y}{2}=a^2,\qquad \frac{z-y}{2}=b^2,$$

此處 $a>0$, $b>0$ 且 $a>b$, $(a,b)=1$.

又

$$a+b\equiv a^2+b^2\equiv z\equiv 1 \pmod 2,$$

故 a, b 中一奇一偶. 而得 (3) 及 (4).

2) 由 (3), (4) 所定之 x, y 適合 (1), (2).

$x^2+y^2=(2ab)^2+(a^2-b^2)^2=(a^2+b^2)^2=z^2$, $x>0$, $y>0$, $z>0$, $2|x$.

若 $(x,y)=d$, 則

$$d\mid y=a^2-b^2,\qquad d\mid z=a^2+b^2.$$

故 $d|2(a^2,b^2)$. 因 $(a,b)=1$, 故 $d=1$ 或 2. 但 a 及 b 中一奇一偶, 故 y 爲奇數,即 $d\neq 2$, 所以 $d=1$.

3) 若 a_1, b_1 及 a, b 表同一解,則

$$\frac{z+y}{2}=a_1^2=a^2,\qquad \frac{z-y}{2}=b_1^2=b^2.$$

故 $a_1=a$, $b_1=b$ (因 a_1, b_1 皆爲正數),而得唯一性.

如以 z^2 除 (1) 式, 並命 $\xi=\frac{x}{z}$, $\eta=\frac{y}{z}$, 則本節所討論之問題,一變而爲: 求圓周

$$\xi^2+\eta^2=1$$

上之有理點(所謂有理點者乃指其坐標皆爲有理數). 換言之,本節證得,單位圓上有有理點

$$\xi=\frac{2ab}{a^2+b^2},\qquad \eta=\frac{a^2-b^2}{a^2+b^2};$$

其數無窮. 今推廣此問題. 即問任一二次曲線上有無窮個有理點否? 此說並不眞實. 例如: 雙曲線

$$\xi^2 - 3\eta^2 = 2$$

上並無有理點. 蓋若命 $\xi = \frac{x}{z}$, $\eta = \frac{y}{z}$, $(x, y, z) = 1$, 則一變而爲求

$$x^2 - 3y^2 = 2z^2$$

之整數解的問題. 取 3 爲模,則

$$x^2 \equiv 2z^2 \pmod 3).$$

由此可得 $3 \mid x$, $3 \mid z$. 更由前式 $3 \mid y$, 此與 $(x, y, z) = 1$ 相違背. 但吾人有次之定理:

定理 2. 在非直線的有有理係數的二次曲線上如有一有理點, 則有無窮個有理點.

證: 可以假定所經過之有理點卽爲原點 (不然, 用平行移動 $\xi' = \xi + \xi_0$, $\eta' = \eta + \eta_0$, 卽得所需). 此二次曲線可以寫成

$$S_2(\xi, \eta) + S_1(\xi, \eta) = 0,$$

此處 $S_i(\xi, \eta)$ 爲 ξ 及 η 之 i 次齊次式. 若 $S_1(\xi, \eta)$ 恆等於 0, 則原二次曲線爲兩條直線. 若 $S_2(\xi, \eta)$ 恆等於 0, 則原曲線爲一直線,故 $S_1(\xi, \eta)$, $S_2(\xi, \eta)$ 均不能恆等於 0.

今命 $\eta = \zeta\xi$, 則

$$\xi S_2(1, \zeta) + S_1(1, \zeta) = 0.$$

而得

$$\xi = -S_1(1, \zeta)/S_2(1, \zeta), \qquad \eta = -\zeta S_1(1, \zeta)/S_2(1, \zeta).$$

故有無窮個有理點.

定理 3. 設 A, B, C 爲不全爲零之有理數. 若 $B^2 - 4AC$ 爲一平方數, 則二次曲線

$$A\xi^2 + B\xi\eta + C\eta^2 + D\xi + E\eta + F = 0 \tag{5}$$

上有無窮個有理點. 換言之, 若一雙曲線之漸近線之方程有有理係數, 則此雙曲線上有無窮個有理點;又一拋物線上也有無窮個有理點.

證: 命 $B^2 - 4AC = L^2$, 則

$$A\xi^2 + B\xi\eta + C\eta^2 = A\left(\left(\xi + \frac{B}{2A}\eta\right)^2 + \left(\frac{C}{A} - \frac{B^2}{4A^2}\right)\eta^2\right) =$$

$$= A\left(\xi + \frac{B}{2A}\eta - \frac{L}{2A}\eta\right)\left(\xi + \frac{B}{2A}\eta + \frac{L}{2A}\eta\right).$$

若 $L \neq 0$, 命

$$\xi' = \xi + \frac{B+L}{2A}\eta, \qquad \eta' = \xi - \frac{-B+L}{2A}\eta,$$

解出 ξ 及 η 代入 (5) 式可得

$$A\xi'\eta' + D'\xi' + E'\eta' + F' = 0.$$

解出 ξ' 得

$$\xi' = -(E'\eta' + F')/(A\eta' + D').$$

故顯然 (5) 有無窮個有理解.

若 $L = 0$, 命 $\xi' = \xi - \frac{B}{2A}\eta$, $\eta' = -\eta$, 則得

$$A\xi'^2 + D'\xi' + E'\eta' + F' = 0.$$

若 $E' \neq 0$, 則 $\eta' = -(A\xi'^2 + D'\xi' + F')/E'$. 故有無窮個有理點.

若 $E' = 0$, 則原曲線並非二次曲線.

附註: 由定理 2 及 3, 推出下列的問題. 命

$$f(x_1, x_2, x_3, \cdots, x_n) = 0 \tag{6}$$

爲一 $x_1, \cdots, x_n$ 之整係數二次齊次式 (不能分解爲一次式之積). 今問有無窮個整點適合此式之條件? 由定理 2 可知當 $n \geqslant 3$, 則如其上有一非原點之整點, 其上卽有無窮個整點. 但何時其上可有一整點? 例如:

$$x_1^2 + x_2^2 + x_3^2 + \cdots + x_n^2 = 0$$

其上決無原點以外之整點. 故建議吾人必須假定 $f(\xi_1, \cdots, \xi_n) = 0$ 有實數軌跡. 吾人可證明如合此條件, 且 $n \geqslant 5$, 則 (6) 上有一整點. 亦卽有無窮個整點 (此乃 Mayer 之定理本書不論證之). 但當 $n = 4$, 此定理不能成立. 蓋若

$$x_1^2 + x_2^2 + x_3^2 - 7x_4^2 = 0,$$

則可假定 $(x_1, x_2, x_3, x_4) = 1$. 又得

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod 8,$$

而 $x^2 \equiv 0, 1, 4 \pmod 8$. 由此式可知 $2 \mid (x_1, x_2, x_3, x_4)$. 此與假定相違背.

習題 1. 解不定方程

$$x^2 + y^2 = z^4,$$

並證明其解能適合

$$x>0,\quad y>0,\quad z>0,\quad (x,y)=1,\quad 2\mid x$$

者，由次式與之：

$$x=4ab\,(a^2-b^2),\quad y=|\,a^4+b^4-6a^2b^2\,|,\quad z=a^2+b^2,$$
$$a>0,\quad b>0,\quad (a,b)=1,\quad a+b\equiv 1 \pmod 2).$$

習題 2. 證明

$$x^4+y^2=z^2,\quad 2\mid x,\quad y>0,\quad z>0,\quad (x,y)=1$$

之解答為

$$x=2ab,\quad y=|\,4a^4-b^4\,|,\quad z=4a^4+b^4,$$
$$(a,b)=1,\quad a>0,\quad b>0,\quad 2\nmid b.$$

習題 3. 證明不定方程 $x^2+(x+1)^2=y^2$ 之解為

$$x=\frac{1}{4}\Big((1+\sqrt{2})^{2n+1}+(1-\sqrt{2})^{2n+1}-2\Big),$$
$$y=\frac{1}{2\sqrt{2}}\Big((1+\sqrt{2})^{2n+1}-(1-\sqrt{2})^{2n+1}\Big),$$

且無其他解。

習題 4. 關於商高定理 $3^2+4^2=5^2$ 有次之推廣：$10^2+11^2+12^2=$ $=13^2+14^2$. 一般言之,證明

$$(2n^2+n)^2+(2n^2+n+1)^2+\cdots+(2n^2+2n)^2=$$
$$=(2n^2+2n+1)^2+\cdots+(2n^2+3n)^2.$$

習題 5. 求證下列諸曲線上有無窮個有理點：

(a) $\eta^2(d-\xi)=\xi^3$,

(b) $\eta(\xi^2+\eta^2)=d(\eta^2-\xi^2)$,

(c) $\xi^3+\eta^3-3\,d\xi\eta=0$,

(d) $(\xi^2-d^2)^2-\alpha\eta^2(2\eta+3d)=0$.

習題 6. 定出所有的三角形，其邊及面積皆為有理數者.

習題 7. 研究不定方程 $x^2+y^2+z^2=w^2$ 之解.

習題 8. 設整數 a,b,c 不同號，$abc\neq 0$，且 abc 無平方因子,則不定方程

$$ax^2+by^2+cz^2=0$$

有不全爲零的整數解的充要條件是: $-bc$ 是 a 的二次剩餘, $-ac$ 是 b 的二次剩餘, $-ab$ 是 c 的二次剩餘.

§7. Fermat 猜測.

Fermat 曾推測當 $n \geqslant 3$ 時

$$x^n + y^n = z^n, \quad x > 0, \quad y > 0, \quad z > 0$$

無整數解. 此定理是否眞實, 至今仍爲疑案. 所可言者, 祇於 $2 < n < 619$ 時, 此定理已經證明. 卽此甚微之結果, 亦已耗却頗多數學家之腦汁矣.

欲證此理, 僅需證明此定理當 $n = 4$ 及 n 爲奇素數時眞實卽已足够. 蓋若 n 有一奇素數因子 p, 則有

$$(x^{n/p})^p + (y^{n/p})^p = (z^{n/p})^p.$$

若 n 無奇素數因子, 則 $n = 2^k$, $k \geqslant 2$, 則有

$$(x^{n/4})^4 + (y^{n/4})^4 = (z^{n/4})^4.$$

是以吾人如能證明 $n = 4$ 時之結論, 則整個問題之解決, 將歸於 n 爲奇素數時之情況矣.

定理 1. 無整數能適合

$$x^4 + y^4 = z^2, \quad x > 0, \quad y > 0.$$

證: 設 u 爲最小之整數, 使不定方程

$$x^4 + y^4 = u^2, \qquad x > 0, \qquad y > 0$$

爲可解者. 則 $(x, y) = 1$. 若不然, 則 $\frac{u}{(x, y)^2}$ 將小於 u, 且具同一性質.

同於 §6 之討論, x 及 y 必爲一奇一偶. 設 x 爲偶, 則由定理 6.1,

$$x^2 = 2ab, \quad y^2 = a^2 - b^2, \quad u = a^2 + b^2,$$

$$a > 0, \quad b > 0, \quad (a, b) = 1, \quad a + b \equiv 1 \pmod 2.$$

若 a 偶 b 奇, 則 $y^2 \equiv -1 \pmod 4$, 此不可能. 故 b 偶 a 奇. 命 $b=2c$, 則

$$\left(\frac{1}{2}x\right)^2 = ac, \qquad (a, c) = 1.$$

因之

$$a = d^2, \quad c = f^2, \quad d > 0, \quad f > 0, \quad (d, f) = 1, \quad 2 \nmid d.$$

故

$$y^2 = a^2 - b^2 = d^4 - 4f^4.$$

即

$$(2f^2)^2 + y^2 = (d^2)^2$$

且 $(2f^2, y, d^2) = 1$.

再由定理 6.1, 得

$$2f^2 = 2lm, \quad d^2 = l^2 + m^2, \quad l > 0, \quad m > 0, \quad (l, m) = 1.$$

由

$$f^2 = lm, \qquad (l, m) = 1$$

可立得

$$l = r^2, \quad m = s^2, \quad (r > 0, s > 0)$$

故

$$d^2 = r^4 + s^4.$$

但

$$d \leqslant d^2 = a \leqslant a^2 < a^2 + b^2 = u.$$

d 較 u 更小, 與假定相違背. 故得定理.

此法乃 Fermat 所創之無窮遞降法 (Méthode d'infinite decent). 其證法之邏輯步驟如次:

(1) 若一命題 $P(n)$ 對若干正整數 n 爲眞,則在此諸 n 中,必有一最小者.

(2) 若 $P(n)$ 爲眞, 則有一正整數 $n' < n$, 使 $P(n')$ 亦眞.

若此二步已證, 則命題 $P(n)$ 決不眞實.

習題 1. 證明次諸不定方程無解:

(a) $x^4 + 4y^4 = z^2, \quad x > 0, \quad y > 0,$

(b) $x^4 - y^4 = z^2, \quad y > 0, \quad z > 0,$

(提示: $z^4 + 4(xy)^4 = (x^4 + y^4)^2$.)

(c) $x^4 - y^4 = 2z^2, \quad y > 0, \quad z > 0,$

(d) $x^4 - y^4 = pz^2, \quad z > 0,$

此處 p 爲素數, $p \equiv 3 \pmod 8$.

習題 2. 證明不定方程

$$x^4 - 2^y z^4 = 1$$

無正整數解.

習題 3. 證明不定方程組

$$x^2+y^2=z^2$$
$$y^2+z^2=t^2$$

無不全爲 0 的整數解。

習題 4. 利用上題證明：三邊皆爲有理整數的直角三角形之面積不可能是一完全平方數.

習題 5. 證明對任一正整數 $n>2$, 不定方程

$$y_n^n=y_{n-1}^{n-1}+y_{n-2}^{n-2}+\cdots+y_2^2$$

有無窮多組正整數解.

(提示：$2^6=2^5+1^4+3^3+2^2$.)

習題 6. 求出不定方程

$$2x^n=z^{n-1}$$

的全部正整數解.

習題 7. 設 l, m, n 爲正整數, $(lm, n)=(ln, m)=(mn, l)=1$, 則不定方程

$$x^l+y^m=z^n$$

有無窮多組正整數解.

(見數學通報 1955 年 8 月號, 同郝, 方程 $a^p+b^q=c^r$ 之整數解.)

習題 8. 若 $x^n+y^n=z^n$ 無整數解, 則

$$x^{2n}+y^{2n}=z^2$$

也無整數解.

§8. Марков 方程.

在 §10.5 中, 吾人曾定義不定方程

$$x^2+y^2+z^2=3xyz \tag{1}$$

之解爲 Марков 數, 並述及 Марков 數與連分數之關係. 今往討論此不定方程.

定理 1. 若 x_0, y_0, z_0 爲 (1) 式之解, 則

$$x_0,\ y_0,\ 3x_0y_0-z_0 \tag{2}$$

亦爲 (1) 式之解.

證: $x_0^2+y_0^2+(3x_0y_0-z_0)^2=$

$$= x_0^2 + y_0^2 + z_0^2 - 6x_0y_0z_0 + 9x_0^2y_0^2 =$$

$$= -3x_0y_0z_0 + 9x_0^2y_0^2 = 3x_0y_0(3x_0y_0 - z_0).$$

定理 2. 凡 (1) 式之解, 可由定理 1 中之方法, 由 $x = y = z = 1$ 一解以得出之.

證: 1) 若 $x = y = z$, 則顯然 $x = y = z = 1$.

2) 若 $x = y \neq z$, 則

$$2x^2 + z^2 = 3x^2 z.$$

由此顯然 $x^2 | z^2$, 卽 $x | z$. 命 $z = wx$, 則得

$$2 + w^2 = 3wx, \quad (w > 0).$$

卽 $w | 2$. 故 $w = 1$ 或 2. 但 $x \neq z$, 故 $w \neq 1$. 若 $w = 2$, 則

$$x = 1, \quad y = 1, \quad z = 2 \quad (= 3 \cdot 1 \cdot 1 - 1).$$

此解顯然由 (1, 1, 1) 經定理 1 得之.

3) 今可假定

$$x < y < z.$$

如能由此證明 $3xy - z < z$, 則吾人可使 $x + y + z$ 之值逐步變小, 經有限步後, 必至 x, y, z 中之二者 (或三者) 相等之步驟, 卽歸入 1) 或 2) 矣. 今往證明此點.

由

$$z^2 - 3xyz + x^2 + y^2 = 0,$$

可知

$$2z = 3xy \pm \sqrt{9x^2y^2 - 4(x^2 + y^2)}.$$

若

$$2z = 3xy - \sqrt{9x^2y^2 - 4(x^2 + y^2)},$$

則由 $8x^2y^2 - 4x^2 - 4y^2 = 4x^2(y^2 - 1) + 4y^2(x^2 - 1) > 0$ 可知

$$2z < 3xy - xy = 2xy.$$

卽

$$z < xy.$$

但

$$3xyz = x^2 + y^2 + z^2 < 3z^2,$$

卽 $xy < z$，此與前者相矛盾，故祇能

$$2z = 3xy + \sqrt{9x^2y^2 - 4(x^2 + y^2)}.$$

是以

$$2z > 3xy.$$

卽合所需.

例. 應用定理 1 於 1, 1, 1 可得

$$1, 1, 2.$$

再應用定理 1 得

$$1, 5, 13; \qquad 2, 5, 29.$$

繼行此法得下表 ($x \leqslant y \leqslant z < 1000$):

z	1	2	5	13	29	34	89	169	194	233	433	610	985
y	1	1	2	5	5	13	34	29	13	89	295	233	169
x	1	1	1	1	2	1	1	2	5	1	5^2	1	2

注意: 此亦一遞降法也. 幸有一解 $x = y = z = 1$, 無法再降. 故 Fermat 之"無窮遞降法"有兩種用法: 一可用以證明無解, 一可用以證明有無窮個解也.

習題 1. 推廣上法以討論不定方程

$$x_1^2 + x_2^2 + \cdots + x_n^2 = n\, x_1 \cdots x_n.$$

習題 2. 求出

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 4x_1 x_2 x_3 x_4, \quad x_1 \leqslant x_2 \leqslant x_3 \leqslant x_4 \leqslant 100$$

之諸解.

習題 3.

$$2x^4 - y^4 = z^2$$

有無窮多解.

§9. 解方程 $x^3 + y^3 + z^3 + w^3 = 0$.

在論述本節之前，先述一具體例子: 1729 乃最小之正整數，可以兩種方法表爲二立方之和者. 卽

$$1729 = 10^3 + 9^3 = 12^3 + 1^3.$$

但天地間能用二法表爲二立方和者,不止此例. 如:

$$2^3 + 34^3 = 15^3 + 33^3, \quad 9^3 + 15^3 = 2^3 + 16^3$$

皆然. 且更有進於此者

$$70^3 + 560^3 = 98^3 + 552^3 = 315^3 + 525^3,$$

$$121170^3 + 969360^3 = 545275^3 + 908775^3 =$$

$$= 342738^3 + 955512^3 = 336455^3 + 956305^3.$$

又有

$$3^3 + 4^3 + 5^3 = 6^3, \quad 1^3 + 6^3 + 8^3 = 9^3.$$

故解不定方程

$$x^3 + y^3 + z^3 + w^3 = 0$$

乃一有趣味之問題. 惜者吾人迄未能得其諸整數解答之公式. 但 Euler-Binet 有下之方法以表出其所有的有理數解.

定理 1. $W^3 + 3W(X^2 + Y^2 + Z^2) + 6XYZ = 0$ 之有理數解答爲

$$W = -6\rho abc, \quad X = \rho a(a^2 + 3b^2 + 3c^2),$$

$$Y = \rho b(a^2 + 3b^2 + 9c^2), \quad Z = 3\rho c(a^2 + b^2 + 3c^2),$$

此處 $(a, b, c) = 1$, 且 ρ 爲有理數.

證: 用行列式可將該式寫成

$$\begin{vmatrix} W & 3Z & -3Y \\ -Z & W & 3X \\ Y & -X & W \end{vmatrix} = 0.$$

故必有整數 a, b, c 不全爲 0, 且 $(a, b, c) = 1$, 使

$$Wa + 3Zb - 3Yc = 0,$$

$$-Za + Wb + 3Xc = 0,$$

$$Ya - Xb + Wc = 0.$$

由此聯立方程解出 X, Y, Z, W, 立得

$$W = -6\rho abc$$

等, 如題所云.

命

$$\left.\begin{aligned} W&=\frac{1}{2}(\alpha+\beta+\gamma+\delta), & X&=\frac{1}{2}(\alpha+\beta-\gamma-\delta),\\ Y&=\frac{1}{2}(\alpha-\beta+\gamma-\delta), & Z&=\frac{1}{2}(\alpha-\beta-\gamma+\delta),\end{aligned}\right\} \tag{1}$$

則得

$$(\alpha+\beta+\gamma+\delta)^3+3(\alpha+\beta+\gamma+\delta)[(\alpha+\beta-\gamma-\delta)^2+(\alpha-\beta+\gamma-\delta)^2+$$
$$+(\alpha-\beta-\gamma+\delta)^2]+6(\alpha+\beta-\gamma-\delta)(\alpha-\beta+\gamma-\delta)(\alpha-\beta-\gamma+\delta)=0,$$

卽

$$\alpha^3+\beta^3+\gamma^3+\delta^3=0. \tag{2}$$

解 (1), 可得

$$\alpha=\frac{1}{2}(W+X+Y+Z), \quad \beta=\frac{1}{2}(W+X-Y-Z),$$

$$\gamma=\frac{1}{2}(W-X+Y-Z), \quad \delta=\frac{1}{2}(W-X-Y+Z),$$

由定理 1 可得 (2) 式之諸解.

定理 2. 任與一正整數 r, 必有一數 N 存在, 可以用 r 種方法表爲二立方之和.

證: 設 ξ_1, η_1 爲給定的二有理數. 令

$$X=\frac{\xi_1(\xi_1^3+2\eta_1^3)}{\xi_1^3-\eta_1^3}, \qquad Y=\frac{\eta_1(2\xi_1^3+\eta_1^3)}{\xi_1^3-\eta_1^3},$$

$$\xi_2=\frac{X(X^3-2Y^3)}{X^3+Y^3}, \qquad \eta_2=\frac{Y(2X^3-Y^3)}{X^3+Y^3},$$

則得

$$X^3-Y^3=\xi_1^3+\eta_1^3, \qquad \xi_2^3+\eta_2^3=X^3-Y^3. \tag{3}$$

由是得

$$\xi_1^3+\eta_1^3=\xi_2^3+\eta_2^3,$$

$$\frac{X}{Y}=\frac{\xi_1}{2\eta_1}\left(1+2\left(\frac{\eta_1}{\xi_1}\right)^3\right)\left(1+\frac{1}{2}\left(\frac{\eta_1}{\xi_1}\right)^3\right)^{-1},$$

$$\frac{\xi_2}{\eta_2}=\frac{X}{2Y}\left(1-2\left(\frac{Y}{X}\right)^3\right)\left(1-\frac{1}{2}\left(\frac{Y}{X}\right)^3\right)^{-1}.$$

設 $0<\frac{\eta_1}{\xi_1}<\varepsilon<\frac{1}{4}$, 則

$$0<\frac{X}{Y}-\frac{\xi_1}{2\eta_1}=\frac{\frac{3}{4}\left(\frac{\eta_1}{\xi_1}\right)^2}{1+\frac{1}{2}\left(\frac{\eta_1}{\xi_1}\right)^3}<\frac{3}{4}\left(\frac{\eta_1}{\xi_1}\right)^2<\frac{3}{4}\varepsilon^2,$$

於是 $\frac{X}{Y}>\frac{\xi_1}{2\eta_1}>\frac{1}{2\varepsilon}$，亦卽 $\frac{Y}{X}<2\varepsilon$. 又

$$\left|\frac{\xi_2}{\eta_2}-\frac{X}{2Y}\right|=\frac{\frac{3}{4}\left(\frac{Y}{X}\right)^2}{1-\frac{1}{2}\left(\frac{Y}{X}\right)^3}<\frac{3}{4}\left(\frac{Y}{X}\right)<\frac{3}{2}\varepsilon.$$

所以

$$\left|\frac{\xi_2}{\eta_2}-\frac{\xi_1}{4\eta_1}\right|\leqslant\left|\frac{\xi_2}{\eta_2}-\frac{X}{2Y}\right|+\frac{1}{2}\left|\frac{X}{Y}-\frac{\xi_1}{2\eta_1}\right|<2\varepsilon.$$

而

$$\frac{\xi_2}{\eta_2}>\frac{\xi_1}{4\eta_1}-2\varepsilon>\frac{1}{8\varepsilon},\qquad \frac{\eta_2}{\xi_2}<8\varepsilon.$$

依上法進行，可得

$$\left|\frac{\xi_3}{\eta_3}-\frac{\xi_2}{4\eta_2}\right|<2^4\varepsilon,\left|\frac{\xi_4}{\eta_4}-\frac{\xi_3}{4\eta_3}\right|<2^7\varepsilon,\cdots,$$

$$\left|\frac{\xi_{s+1}}{\eta_{s+1}}-\frac{\xi_s}{4\eta_s}\right|<2^{1+3(s-1)}\varepsilon,$$

祇須 $2^{3(s-1)}\varepsilon<\frac{1}{4}$.

故若取 $\frac{\eta_1}{\xi_1}$ 很小，可得一列數對 (ξ_1,η_1)，…，(ξ_r,η_r) 使

$$\xi_1^3+\eta_1^3=\xi_2^3+\eta_2^3=\cdots=\xi_r^3+\eta_r^3,$$

且比値

$$\frac{\xi_1}{\eta_1},\ 4\frac{\xi_2}{\eta_2},\cdots,4^{r-1}\frac{\xi_r}{\eta_r}$$

之比大致相等．故 ξ_s/η_s 各各不等．以公分母乘之，卽得所求．

習題 1. $\alpha^3+\beta^3+\gamma^3+\delta^3=0$ 之有理解可由

$$\alpha=\sigma(-(\xi-3\eta)(\xi^2+3\eta^2)+1),\quad \beta=\sigma((\xi+3\eta)(\xi^2+3\eta^2)-1),$$
$$\gamma=\sigma((\xi^2+3\eta^2)^2-(\xi+3\eta)),\qquad \delta=\sigma((\xi^2+3\eta^2)^2-(\xi-3\eta))$$

表之，此處 ξ,η 爲有理數．

若 $\sigma=1$, ξ 及 η 爲整數，可得出 $x^3+y^3+z^3+w^3=0$ 之無窮個整數解，但此並不包括所有的整數解．試證

$$\alpha=1,\quad \beta=12,\quad \gamma=-10,\quad \delta=-9$$

卽其一例．

習題 2. 證恆等式

$$y^{12}=(9x^4)^3+(3xy^3-9x^4)^3+(y^4-9x^3y)^3.$$

因之得

$$5^{12}=9^3+366^3+580^3=144^3+606^3+265^3.$$

習題 3. 由上習題，證明有 n 存在，使

$$n=x^3+y^3+z^3,\quad x\geqslant 0,\quad y\geqslant 0,\quad z\geqslant 0$$

之解數 $>\frac{1}{3}n^{\frac{1}{12}}$.

習題 4. 證明

$$(3a^2+5ab-5b^2)^3+(4a^2-4ab+6b^2)^3+(5a^2-5ab-3b^2)^3=(6a^2-4ab+4b^2)^3.$$

§10. 三次曲面之有理點．

本節所討論的三次曲面非錐面與柱面．

以 δ^3 除上節之 (2) 式，再命 $\xi=-\alpha/\delta$, $\eta=-\beta/\delta$, $\zeta=-\gamma/\delta$, 則得

$$\xi^3+\eta^3+\zeta^3=1. \tag{1}$$

換言之，由 §9 之結果可以推出：三次曲面 (1) 上有無窮個有理點．本節將討論最普遍的三次曲面．

爲了介紹一比較困難之方法，特先做若干特例：

定理 1. 若 $C\neq 0$, 則三次曲面

$$\zeta^2=\xi^3+A\xi+B+C\eta^2 \tag{2}$$

上有無窮個有理點，此處 A, B, C 皆爲有理數．

證：以

$$\xi=\eta^2+T\eta,\qquad \zeta=\eta^3+\lambda\eta^2+\mu\eta+\nu \tag{3}$$

代入 (2) 式，則得

$$(\eta^3+\lambda\eta^2+\mu\eta+\nu)^2=(\eta^2+T\eta)^3+A(\eta^2+T\eta)+B+C\eta^2. \tag{4}$$

比較 $\eta^6, \eta^5, \eta^4, \eta^3$ 之係數，得

$$2\lambda = 3T, \quad \lambda^2 + 2\mu = 3T^2, \quad 2(\nu + \lambda\mu) = T^3.$$

解得

$$\lambda = \frac{3}{2}T, \quad \mu = \frac{3}{8}T^2, \quad \nu = -\frac{1}{16}T^3.$$

以此代入 (4) 式，得出一 η 之二次式

$$L\eta^2 + M\eta + N = 0, \tag{5}$$

此處

$$L = A + C - \mu^2 - 2\lambda\nu = A + C + \frac{3}{64}T^4,$$

$$M = AT - 2\mu\nu = AT + \frac{3}{64}T^5,$$

$$N = B - \nu^2 = B - \frac{1}{256}T^6.$$

(5) 之判別式

$$\varDelta = M^2 - 4LN = \left[\left(\frac{3}{64}\right)^2 + \frac{3}{64}\cdot\frac{1}{64}\right]T^{10} + \cdots =$$

$$= \frac{3}{1024}T^{10} + \cdots,$$

故 $\varDelta$ 決非一有理係數多項式之平方. 故 (5) 式之解可表爲

$$\eta = \beta_1 \pm \beta_2\sqrt{\varDelta}, \quad \beta_1 = -\frac{M}{2L}, \quad \beta_2 = \frac{1}{2L}.$$

代入 (3) 式可得

$$\xi = \alpha_1 \pm \alpha_2\sqrt{\varDelta}, \quad \zeta = \gamma_1 \pm \gamma_2\sqrt{\varDelta},$$

此處

$$\alpha_2 = (2\beta_1 + T)\beta_2 = \frac{LT-M}{2L^2} = \frac{CT}{2L^2} \neq 0.$$

命

$$\frac{\xi-\alpha_1}{\alpha_2} = \frac{\eta-\beta_1}{\beta_2} = \frac{\zeta-\gamma_1}{\gamma_2} = \sigma. \tag{6}$$

以此代入 (2) 式，得一 σ 之三次方程，其各項係數皆爲 T 之有理函數，而其首項係數 α_2^3 不等於零. 又已知 $\pm\sqrt{\varDelta}$ 爲此式的二根，故另一根 σ_0 必爲 T 之有理函數. 以此代入 (6) 式，可將 ξ, η, ζ 表爲 T 之有理函數. 但最後尚須證明：由此所得之 ξ, η, ζ 不能均爲常數，否則，吾人並未得出無窮個有理

點也. 若 η 是不等於零的常數,則 $\xi = \eta^2 + T\eta$ 非常數,蓋若 $\eta = 0$, 則由 (3), 得 $\xi = 0$ 及 $\zeta = \nu = -\frac{1}{16}T^3$, 又由 (2) 知此乃不可能之事. 故由此可見, 如以 σ_0 代入 (6) 式, 則 ξ, η, ζ 均爲 T 之有理函數, 而不能同時均爲常數. 定理得證.

定理 2. 設 $f(\xi, \eta)$ 爲一有有理係數之三次多項式, 但不能用一一次變形變爲僅有一個變數之多項式, 則三次曲面

$$\zeta^2 = f(\xi, \eta) \tag{7}$$

上有無窮個有理點.

證: 命 $f_3(\xi, \eta)$ 爲 $f(\xi, \eta)$ 中之三次齊次部分.

1) 若 $f_3(\xi, 1) = 0$ 有一有理根 a (同法可以討論 $f_3(1, \eta)$ 有有理根之情況), 則 $f(\xi + a\eta, \eta) = g(\xi, \eta)$ 中無 η^3 之項. 故經變換 $\xi \to \xi + a\eta$, $\eta \to \eta$, $\zeta \to \zeta$ 之後, (7) 式可以寫成:

$$\zeta^2 = L_1(\xi)\,\eta^2 + L_2(\xi)\,\eta + L_3(\xi). \tag{8}$$

此處 L_1, L_2, L_3 爲 ξ 之一, 二, 三次多項式. 命

$$L_1(\xi) = \alpha\xi + \beta.$$

若 $\alpha \neq 0$, 則可取 ξ 使 $\alpha\xi + \beta = \delta^2 \neq 0$, 如此, 則由定理 6.3 可得定理.

若 $\alpha = 0$ 及 $\beta = 0$, (8) 乃 η 之一次式. 解出 η, 即得定理. 今假定 $\alpha = 0$, $\beta \neq 0$, 則 (8) 式可以寫成

$$\zeta^2 = \alpha_1\,\xi^3 + \alpha_2\,\xi^2\,\eta + \beta_1\,\xi^2 + \beta_2\,\xi\eta + \beta\eta^2 + \cdots. \tag{9}$$

此處 $\cdots$ 代表 ξ 及 η 之一次式.

設 $\alpha_2 \neq 0$. 命 $\alpha_1\xi + \alpha_2\eta = \lambda$, 則得

$$\zeta^2 = \lambda\,\xi^2 + \beta_1\,\xi^2 + \beta_2\,\xi\left(\frac{\lambda - \alpha_1\,\xi}{\alpha_2}\right) + \beta\left(\frac{\lambda - \alpha_1\,\xi}{\alpha_2}\right)^2 + \cdots =$$

$$= (\lambda + \beta_1 - \beta_2\,\alpha_1/\alpha_2 + \beta\,\alpha_1^2/\alpha_2^2)\,\xi^2 + \cdots.$$

取 $\lambda = 1 - \beta_1 + \beta_2\,\alpha_1/\alpha_2 - \beta\,\alpha_1^2/\alpha_2^2$, 則得

$$\zeta^2 - \xi^2 = (\zeta - \xi)\,(\zeta + \xi) = A\xi + B.$$

由定理 6.3 此曲線上有無窮個有理點.

故未能解決者爲 $\alpha_2 = 0$ 之情況, 此時 $\alpha_1 \neq 0$, 否則 $\zeta^2 = f(\xi, \eta)$ 非三

次曲面. 於是

$$\zeta^2 = \alpha_1 \xi^3 + \beta_1 \xi^2 + \beta_2 \xi\eta + \beta\eta^2 + \cdots =$$
$$= \beta\eta^2 + (\beta_2 \xi + \gamma)\,\eta + f(\xi) =$$
$$= \beta\left(\eta + \frac{\beta_2}{2\beta}\,\xi + \frac{\gamma}{2\beta}\right)^2 + g(\xi).$$

此處 $g(\xi)$ 爲 ξ 之三次多項式其首項係數爲 α_1. 換 $\eta+\frac{\beta_2}{2\beta}\xi+\frac{\gamma}{2\beta}$ 爲 η, 則得

$$\zeta^2 = \beta\,\eta^2 + g(\xi).$$

兩邊各以 α_1^2 乘之, 再用一簡單的變換 $\xi' = \alpha_1\xi + A$, $\zeta'=\alpha_1\zeta$ 可將此式化爲 (2) 式. 由定理 1 故得定理.

2) 假定 $f_3(\xi, \eta)$ 無一次有理因子, (7) 式可以寫成

$$\zeta^2 = \alpha\,\xi^3 + f_1(\eta)\,\xi^2 + f_2(\eta)\,\xi + f_3(\eta),$$

此處 f_1, f_2, f_3 是 η 之一, 二, 三次多項式. 以 $\xi-\frac{f_1(\eta)}{3\alpha}$ 代 ξ, 得一新式

$$\zeta^2 = \alpha\,\xi^3 + g_2(\eta)\,\xi + g_3(\eta).$$

兩邊以 α^2 乘之, 再換 $\alpha\zeta$, $\alpha\xi$ 爲 ζ 及 ξ, 則得

$$\zeta^2 = \xi^3 + (A\eta^2 + B\eta + C)\,\xi + D\eta^3 + E\eta^2 + F\eta + G. \tag{10}$$

同定理 1 法, 以

$$\xi = \eta^2 + T\eta, \qquad \zeta = \eta^3 + \lambda\eta^2 + \mu\eta + \nu \tag{11}$$

代入 (10) 式, 得

$$(\eta^3 + \lambda\eta^2 + \mu\eta + \nu)^2 = (\eta^2 + T\eta)^3 + (A\eta^2 + B\eta + C)\,(\eta^2 + T\eta) +$$
$$+ D\eta^3 + E\eta^2 + F\eta + G. \tag{12}$$

定 λ, μ, ν 之值使 (12) 式中 η^5, η^4, η^3 之係數爲零. 如此則得一 η 之二次方程式

$$L\eta^2 + M\eta + N = 0,$$

此處 L 並非爲零 (讀者自證). 解此方程得

$$\eta = \beta_1 \pm \beta_2\sqrt{\Delta},$$

此處 β_1, β_2 及 Δ 爲 T 之有理函數. 以此代入 (11) 則

$$\xi = \alpha_1 \pm \alpha_2\sqrt{\Delta}, \qquad \zeta = \gamma_1 \pm \gamma_2\sqrt{\Delta}.$$

若 $\Delta = 0$ 則已得所求. 若 $\Delta \neq 0$, 命

$$\frac{\xi-\alpha_1}{\alpha_2} = \frac{\eta-\beta_1}{\beta_2} = \frac{\zeta-\gamma_1}{\gamma_2} = \sigma.$$

以此代入 (10) 式得一 σ 之三次方程式, 其 σ^3 之係數爲

$$\alpha_2^3 + A\beta_2^2\alpha_2 + D\beta_2^3\,(= f_3(\alpha_2, \beta_2)),$$

此非爲零. 此三次方程式之二根已知其爲 $\pm\sqrt{\Delta}$, 故其第三根 σ_0 爲 T 之有理函數. 卽

$$\xi = \alpha_1 + \alpha_2\sigma_0, \quad \eta = \beta_1 + \beta_2\sigma_0, \quad \zeta = \gamma_1 + \gamma_2\sigma_0$$

在三次曲面 (10) 上,並可證明 ξ, η, ζ 不能均爲常數,其證明一如定理 1. 於是定理得到證明.

定理 3. 命 $S_2(\xi, \eta, \zeta)$ 及 $T_2(\xi, \eta, \zeta)$ 爲 ξ, η, ζ 之二次齊次式,則三次曲面

$$\zeta S_2(\xi, \eta, \zeta) + T_2(\xi, \eta, \zeta) + \zeta = 0 \tag{13}$$

上有無窮個有理點.

證: 以 $f(\xi, \eta, \zeta)$ 表 (13) 之左邊, 則

$$f(\xi, \eta, \zeta) = (\alpha_1 + \alpha_2\zeta)\xi^2 + (\beta_1 + \beta_2\zeta)\xi\eta + (\gamma_1 + \gamma_2\zeta)\eta^2 + g(\xi, \eta, \zeta), \tag{14}$$

此處 $g(\xi, \eta, \zeta)$ 乃 ξ 及 η 之一次式. 於定理 6.3 中取 $A = \alpha_1 + \alpha_2\zeta$, $B = \beta_1 + \beta_2\zeta$, $C = \gamma_1 + \gamma_2\zeta$, 則

$$B^2 - 4AC = (\beta_1 + \beta_2\zeta)^2 - 4(\alpha_1 + \alpha_2\zeta)(\gamma_1 + \gamma_2\zeta).$$

若 $\alpha_2 \neq 0$ (或 $\gamma_2 \neq 0$), 則取 $\zeta = -\frac{\alpha_1}{\alpha_2}\left(\text{或 } \zeta = -\frac{\gamma_1}{\gamma_2}\right)$, 故 B^2-4AC 爲一平方數. 若 $\alpha_2 = \gamma_2 = 0$, 而 $\beta_2 \neq 0$, 則 $\delta^2 = (\beta_1+\beta_2\zeta)^2 - 4\alpha_1\gamma_1$ 亦有有理解 (再用定理 6.3). 但有一情況必須注意, 卽若以 $\zeta = -\frac{\alpha_1}{\alpha_2}$ 代入 (14) 後, 所有的 $\xi^2, \xi\eta, \eta^2$ 之係數皆等於零. 此時若 ξ 及 η 之係數不皆爲零, 則可將 ξ (或 η) 表爲 $\eta, -\frac{\alpha_1}{\alpha_2}\left(\text{或 } \xi, -\frac{\alpha_1}{\alpha_2}\right)$ 之有理函數,定理依然成立. 若 ξ 及 η 之係數亦全爲零, 則

$$f(\xi, \eta, \zeta) = (\alpha_1 + \alpha_2\zeta)(\xi^2 + A\xi\eta + B\eta^2 + (C + D\zeta)\xi + \\ + (E + F\zeta)\eta + G + H\zeta + J\zeta^2) + K.$$

於 (13) 式中如命 $\zeta = 0$, 得 $f(\xi, \eta, 0)$ 爲 ξ 及 η 之二次齊次式, 故在上式中

$C=E=0,\ \alpha_1 G+K=0$，即

$$f(\xi,\eta,\zeta)=(\alpha_1+\alpha_2\zeta)(\xi^2+A\xi\eta+B\eta^2+D\xi\zeta+F\eta\zeta)+P(\zeta),\ P(0)=0. \qquad (15)$$

注意

$$(\xi+\lambda\zeta)^2+A(\xi+\lambda\zeta)(\eta+\mu\zeta)+B(\eta+\mu\zeta)^2+D(\xi+\lambda\zeta)\zeta+F(\eta+\mu\zeta)\zeta=$$
$$=\xi^2+A\xi\eta+B\eta^2+(2\lambda+A\mu+D)\xi\zeta+(A\lambda+2B\mu+F)\eta\zeta+\cdots.$$

若 $A^2\neq 4B$，則可取 λ 及 μ 使 $2\lambda+A\mu+D=0,\ A\lambda+2B\mu+F=0$. 故可假定

$$f(\xi,\eta,\zeta)=(\alpha_1+\alpha_2\zeta)(\xi^2+A\xi\eta+B\eta^2)+g(\zeta),\quad g(0)=0.$$

命

$$\zeta=\frac{1}{Z},\quad \xi=\frac{X}{Z^2(\alpha_1+\alpha_2\zeta)},\quad \eta=\frac{Y}{Z^2(\alpha_1+\alpha_2\zeta)}.$$

則得

$$X^2+AXY+BY^2+Z^4\left(\alpha_1+\frac{\alpha_2}{Z}\right)g\left(\frac{1}{Z}\right)=0.$$

因 $g(0)=0$，故 $Z^4\left(\alpha_1+\frac{\alpha_2}{Z}\right)g\left(\frac{1}{Z}\right)$ 爲 Z 之三次式，此易化爲定理 2 之形式. 故得定理.

若 $A^2=4B$，則 (15) 中代入 $\xi+\frac{A}{2}\eta=\xi',\ \eta=\eta'$，則 $f(\xi,\eta,\zeta)$ 爲 η' 之一次式，故亦得定理.

若 $\alpha_2=\beta_2=\gamma_2=0$，而 $\beta_1^2\neq 4\alpha_1\gamma_1$，則經過變形 $\xi\to\xi+\lambda_1\zeta+\lambda_2\zeta^2$，$\eta\to\eta+\mu_1\zeta+\mu_2\zeta^2$，可使 (14) 式變成

$$\alpha_1\xi^2+\beta_1\xi\eta+\gamma_1\eta^2+f(\zeta)=0,$$

此處 $f(\zeta)=A\zeta^4+B\zeta^3+C\zeta^2+D\zeta$. 再作變換 $\xi=\frac{X}{Z^2},\ \eta=\frac{Y}{Z^2},\ \zeta=\frac{1}{Z}$，可得

$$\alpha_1X^2+\beta_1XY+\gamma_1Y^2+A+BZ+CZ^2+DZ^3=0.$$

再經過一次變換，可使其化爲定理 2 的情形，故得定理.

若 $\alpha_2=\beta_2=\gamma_2=0$，且 $\beta_1^2=4\alpha_1\gamma_1$，則經過一次變換 $\xi'=\alpha_1\xi+$ $+\frac{\beta_1}{2}\eta,\ \eta'=\eta,\ \zeta'=\zeta$ 可使 (14) 式的左邊變爲 η' 的一次式. 於是定理亦得證.

定理 4. 若非錐面及柱面的三次曲面上有一有理點，則有無窮個有理點.

證: 可假定原點卽爲此有理點. 如此則此曲面可以寫成

$$S_3(\xi,\eta,\zeta)+S_2(\xi,\eta,\zeta)+S_1(\xi,\eta,\zeta)=0, \tag{16}$$

此處 $S_i(\xi,\eta,\zeta)$ 爲 ξ,η,ζ 之 i 次齊次式.

1) 若 $S_1(\xi,\eta,\zeta)$ 恆等於 0, 卽

$$S_3(\xi,\eta,\zeta)+S_2(\xi,\eta,\zeta)=0,$$

可得

$$\zeta\, S_3\left(\frac{\xi}{\zeta},\frac{\eta}{\zeta},1\right)+S_2\left(\frac{\xi}{\zeta},\frac{\eta}{\zeta},1\right)=0.$$

卽

$$\zeta=-S_2(\alpha,\beta,1)\,/\,S_3(\alpha,\beta,1).$$

故得定理. 但須注意二事: (1) $S_3(\alpha,\beta,1)$ 恆等於 0, 如此則原曲面非三次者. (2) $S_2(\alpha,\beta,1)$ 恆等於 0, 則原曲面爲一三次曲線及原點所演成之錐面.

2) 若 $S_1(\xi,\eta,\zeta)$ 非恆等於零, 則用變形 $S_1(\xi,\eta,\zeta)\to\zeta$, 可以得出

$$S_3(\xi,\eta,\zeta)+S_2(\xi,\eta,\zeta)+\zeta=0.$$

若 $S_3(\xi,\eta,0)$ 及 $S_2(\xi,\eta,0)$ 均不恆等於 0, 命 $\zeta=0$, 則得

$$S_3(\xi,\eta,0)+S_2(\xi,\eta,0)=0,\quad \eta=-S_2(\xi/\eta,1,0)\,/\,S_3(\xi/\eta,1,0).$$

若 $S_2(\xi,\eta,0)$ 恆等於 0, 則 $S_2(\xi,\eta,\zeta)=\zeta\, L_1(\xi,\eta,\zeta)$. 命 $\frac{1}{\zeta}=Z, \frac{\xi}{\zeta}=$ $=X, \frac{\eta}{\zeta}=Y$, 則得

$$S_3(X,Y,1)+Z\,L_1(X,Y,1)+Z^2=0.$$

卽

$$\left(Z+\frac{1}{2}L_1(X,Y,1)\right)^2=\frac{1}{4}L_1^2(X,Y,1)-S_3(X,Y,1).$$

此乃定理 2 中所討論者. 故得定理.

若 $S_3(\xi,\eta,0)$ 恆等於 0, 命 $S_3(\xi,\eta,\zeta)=\zeta\ T_2(\xi,\eta,\zeta)$, 此卽定理 3 所討論之情況. 故定理已完全證明.

習題 1.*) 求出下列不定方程的全部正整數解:

1) $2^x-3^y=1$,

2) $3^x-2^y=1$.

*) 此諸習題之解法, 並非固定用某一節之方法, 故附於本章之末.

習題 2. 證明不定方程

$$5^x = 2^y + 3^z$$

祇有三組整數解: $x = y = z = 1$; $x = 1,\ y = 2,\ z = 0$; $x = 2,\ y = 4,\ z=2.$

習題 3. 求出不定方程

$$x^y = y^x$$

的全部有理數解.

習題 4. 證明不定方程

$$x^y = y^x + 1$$

祇有二組正整數解: $x = 2,\ y = 1$; $x = 3,\ y = 2$.

習題 5. 求出不定方程

$$(x + 1)^y = x^{y+1} + 1$$

的全部正整數解.

習題 6. 證明 $x = 7,\ y = 20$ 是不定方程

$$1 + x + x^2 + x^3 = y^2$$

唯一的解使 x 爲素數者.

習題 7. 證明不定方程

$$m \tan^{-1} \frac{1}{x} + n \tan^{-1} \frac{1}{y} = k \frac{\pi}{4}$$

祇有四組整數解 $k,m,n,x,y = 1,1,1,2,3$; $1,2,-1,2,7$; $1,2,1,3,7$; $1,4,-1,5,239$. 試利用最後一解以計算 π 之值準確至十萬分之一.

第 十 二 章

二 元 二 次 型

§1. 二元二次型之分類.

定義. 對固定之整數 a, b, c, 二次齊次多項式

$$F = F(x, y) = ax^2 + bxy + cy^2$$

稱爲二元二次型,或簡稱爲型,以 $\{a, b, c\}$ 表示之. 整數

$$d = b^2 - 4ac$$

稱爲此型之判別式.

由此顯然可見

$$d \equiv 0 \text{ 或 } 1 \pmod 4.$$

定理 1. F 可分解爲二整係數一次式之積之必要且充分條件爲 d 爲一平方數.

證: 1) 若 d 爲一平方數及 $a \neq 0$, 則

$$ax^2 + bx + c = a\left(\left(x + \frac{b}{2a}\right)^2 - \frac{d}{4a^2}\right) = 0$$

有有理根,由定理 1.13.2, 可知此式可以分解爲二整係數一次式之積. 若 $a=0$, 顯然有 $F(x, y) = (bx + cy)y$.

2) 若

$$ax^2 + bxy + cy^2 = (rx+sy)(tx+uy),$$

則

$$d = b^2 - 4ac = (st+ru)^2 - 4rt \cdot su =$$
$$= (st-ru)^2.$$

故得定理.

今後常設 d 非平方數.

若 $d<0$, $a>0$, 則

$$4aF=(2ax+by)^2+(4ac-b^2)y^2=$$
$$=(2ax+by)^2-dy^2.$$

顯然對任意 x, y 常有 $F(x,y)\geqslant 0$. 若 $F(x,y)=0$, 則得 $x=y=0$. 此種型稱爲定正型. 又若 $d<0$, $a<0$, 則對任意 x, y 常有 $F\leqslant 0$, 此型稱爲定負型. 以 -1 乘定負型,卽得定正型. 故今後常論定正型,並簡稱爲定型.

若 $d>0$, 則

$$F(1,0)=a, \qquad F(b,-2a)=ab^2-b\cdot b\cdot 2a+c\cdot 4a^2=-da.$$

若 $a\neq 0$, 則此二值一正一負. 若 $c\neq 0$, 同法可得二值一正一負. 若 $a=$ $=c=0$, 則

$$F(1,1)=b, \qquad F(1,-1)=-b,$$

也是一正一負. 故當 $d>0$ 時,型 $F(x,y)$ 能取正值也能取負值. 因此此型名爲不定型.

定義. 若有一整係數變換

$$x=rX+sY, \qquad y=tX+uY, \qquad ru-st=1.$$

變 $F(x,y)$ 爲 $G(X,Y)$, 則謂 F 與 G 相似,以

$$F\sim G$$

表之. 或謂 F 經 $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ 而變爲 G.

更具體些,如命 $F=\{a,b,c\}$, $G=\{a_1,b_1,c_1\}$, 則得

$$a_1=ar^2+brt+ct^2, \tag{1}$$
$$b_1=2ars+b(ru+st)+2ctu=$$
$$=2ars+b(1+2st)+2ctu, \tag{2}$$
$$c_1=as^2+bsu+cu^2. \tag{3}$$

由此立得

$$b_1^2-4a_1c_1=(2ars+b(ru+st)+2ctu)^2-$$
$$-4(ar^2+brt+ct^2)(as^2+bsu+cu^2)=$$
$$=(b^2-4ac)(ru-st)^2=b^2-4ac=d.$$

由此可見,相似之二型之判別式相等.

又若 $d<0$, $a>0$, 則 $a_1=F(r,t)\geqslant 0$. 若 $a_1=0$, 則 $r=t=0$, 此不可能. 故得 $a_1>0$. 換言之,與定正型相似之型也是定正型.

定理 2. (i) $F\sim F$ (自反性),

(ii) 若 $F\sim G$, 則 $G\sim F$ (對稱性),

(iii) 若 $F\sim G$, $G\sim H$, 則 $F\sim H$ (傳遞性).

此定理之證明極易,故從略.

依相似性可以將判別式爲 d 之諸型分爲若干類. 同一類之諸型皆相似,不同類之型絕不相似.

顯然同類諸型所表之整數相同. 蓋若 $k=G(X,Y)$,則 $k=F(rX+sY, tX+uY)$ 故也.

§ 2. 類數有限.

定理 1. 每一類中必有一型適合於

$$|b|\leqslant|a|\leqslant|c|.$$

證: 取 a 爲此類所能表示之諸整數 ($\neq 0$) 中之絕對值最小者. 再命 $\{a_0, b_0, c_0\}$ 爲此類中之任何一型. 則有 r, t 使

$$a=a_0r^2+b_0rt+c_0t^2,$$

且 $(r,t)=1$. 若不然,則 $\frac{a}{(r,t)^2}$ 也可由 $\{a_0, b_0, c_0\}$ 表示,而 $\frac{|a|}{(r,t)^2}<|a|$, 是不可能.

可定 s 及 u 使 $ru-st=1$. 則 $\{a_0, b_0, c_0\}$ 經 $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ 而變爲 $\{a, b', c'\}$. 又變形

$$\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$$

變 $\{a, b', c'\}$ 爲 $\{a, b, c\}$,其中

$$b=2ah+b'.$$

可取整數 h 使

$$|b|\leqslant|a|.$$

因 c 可由 $\{a, b, c\}$ 表出, 而 $\{a, b, c\}$ 與 $\{a_0, b_0, c_0\}$ 同屬於一類中, 故 $|c|\geqslant|a|$. (但須注意 $c\neq 0$, 若 $c=0$, 則 d 爲平方數矣.)

定理 2. 類數有限.

證：1) $d>0$（不定型）．由定理 1 可知

$$|ac| \geqslant b^2 = d + 4ac > 4ac.$$

故 $ac<0$，又

$$4a^2 \leqslant 4\,|ac| = -4ac = d - b^2 \leqslant d,$$

即

$$|a| \leqslant \frac{\sqrt{d}}{2}.$$

又由定理 1，$|b| \leqslant \frac{1}{2}\sqrt{d}$．故 a 及 b 祇有有限個可能性，而 $c=(b^2-d)/4a$ 之值也有限．故得定理．

2) $d<0$（定型）．由定理 1 可知（設 $a>0$）

$$-d = 4ac - b^2 \geqslant 4a^2 - b^2 \geqslant 3a^2,$$

故 $0<a\leqslant\sqrt{\frac{|d|}{3}}$．由定理 1 可得定理．

定理 3. 判別式為 d 之定正型之類數等於適合

$$b^2 - 4ac = d,\quad \begin{cases} -a < b \leqslant a < c \\ \text{或 } 0 \leqslant b \leqslant a = c \end{cases} \tag{1}$$

之整數組 a, b, c 之組數．

證：1) 由定理 1 已知在一類中至少有一型適合於

$$-a \leqslant b \leqslant a \leqslant c$$

（因 a, c 常為正）．比結論中所多出者有次列諸型：

$$-a = b,\quad a<c$$

及

$$-a \leqslant b < 0,\quad a = c.$$

今往證明

$$\{a, -a, c\} \sim \{a, a, c\}$$

及

$$\{a, -b, a\} \sim \{a, b, a\}.$$

因為 $\{a,-a,c\}$ 經 $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ 而變為 $\{a,a,c\}$，而 $\{a,-b,a\}$ 經 $\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ 而變為 $\{a,b,a\}$，故得任一類中必有一型適合於 (1)．

2) 今證其中任何二者不相似．即若

$$\{a, b, c\} \sim \{a', b', c'\}$$

並皆適合於 (1),則 $a = a'$, $b = b'$, $c = c'$.

可設 $a' \leqslant a$. 命 $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ 變 $\{a, b, c\}$ 爲 $\{a', b', c'\}$, 則得

$$a' = ar^2 + brt + ct^2, \tag{2}$$

$$b' = 2ars + b(ru+st) + 2ctu. \tag{3}$$

由前者可知

$$a \geqslant a' \geqslant ar^2 - a|rt| + at^2 = a(|r|-|t|)^2 + a|rt| \geqslant a|rt|, \tag{4}$$

卽

$$|rt| \leqslant 1.$$

若 $|rt| = 1$, 則 $a = a'$. 若不然,則 $rt = 0$, 此時

$$a \geqslant a' \geqslant ar^2 + at^2 = a(r^2+t^2) \geqslant a,$$

故必 $a = a'$.

先設 $c > a$, 則 t 必爲零. 不然, (4) 式中由於 $ct^2 > at^2$, 而得 $a > a$, 此不可能. 故 $t = 0$, $ru = 1$. 由 (3) 式

$$b' = 2ars + b \equiv b \pmod{2a}.$$

因 $-a < b \leqslant a$ 及 $-a = -a' < b' \leqslant a' = a$ 可知 $b = b'$. 由此立得 $c = c'$.

再設 $c' > a'(=a)$,可如上法得出同樣結論.

今尚留待討論者爲 $a = a' = c = c'$ 之情況. 此時必有

$$b = \pm b'.$$

由 $b \geqslant 0$, $b' \geqslant 0$, 故得 $b = b'$.

附註: 對非定型之情況並不如此簡易.

定義. 適合 (1) 之型,謂之已化型.

習題 1. 下表給出 $0 < -d \leqslant 20$ 之所有的已化型.

d	-3	-4	-7	-8	-11	-12		-15		-16		-19	-20	
a	1	1	1	1	1	1	2	1	2	1	2	1	1	2
b	1	0	1	0	1	0	2	1	1	0	0	1	0	2
c	1	1	2	2	3	3	2	4	2	4	2	5	5	3

習題 2. 證明 $d = -48$ 時有四個已化型:

$$\{1, 0, 12\}, \quad \{2, 0, 6\}, \quad \{3, 0, 4\}, \quad \{4, 4, 4\}.$$

§3. Kronecker 符號.

定義. 設 $d \equiv 0$ 或 $1 \pmod 4$ 且非平方數.且設 $m > 0$. Kronecker 符號 $\left(\frac{d}{m}\right)$ 之定義如次:

$$\left(\frac{d}{p}\right) = 0, \qquad 若 \qquad p \mid d;$$

$$\left(\frac{d}{2}\right) = \begin{cases} 1, & 若 \quad d \equiv 1 \pmod 8, \\ -1, & 若 \quad d \equiv 5 \pmod 8. \end{cases}$$

$$\left(\frac{d}{p}\right) = \text{Legendre 符號} \quad (p \text{ 奇素數}, \ p \nmid d).$$

若 $m = \prod_{r=1}^{v} p_r$, p_r 爲素數,則

$$\left(\frac{d}{m}\right) = \prod_{r=1}^{v} \left(\frac{d}{p_r}\right).$$

由此易證: 若 $(d, m) > 1$, 則

$$\left(\frac{d}{m}\right) = 0.$$

若 $(d, m) = 1$, 則

$$\left(\frac{d}{m}\right) = \pm 1.$$

又若 $m_1 > 0$, $m_2 > 0$, 則

$$\left(\frac{d}{m_1 m_2}\right) = \left(\frac{d}{m_1}\right)\left(\frac{d}{m_2}\right).$$

定理 1. 若 $m > 0$, $(m, d) = 1$, 則 Kronecker 符號

$$\left(\frac{d}{m}\right) = \begin{cases} \left(\frac{m}{|d|}\right), & 當 \quad d \text{ 爲奇數}, \\ \left(\frac{2}{m}\right)^b (-1)^{\frac{u-1}{2}\frac{m-1}{2}} \left(\frac{m}{|u|}\right), & 當 \quad d = 2^b u, \quad 2 \nmid u. \end{cases}$$

此處 $\left(\frac{m}{|d|}\right)$, $\left(\frac{2}{m}\right)$, $\left(\frac{m}{|u|}\right)$ 全爲 Jacobi 符號.

證: 1) 設 d 爲奇數,由定義及定理 3.6.5, 可得

$$\left(\frac{d}{m}\right) = \left(\frac{m}{|d|}\right).$$

2) 設 $d=2^b u$, $2\nmid u$, 則必 $b\geqslant 2$, 而此時 m 爲奇數,所以

$$\left(\frac{d}{m}\right)=\left(\frac{2}{m}\right)^b\left(\frac{u}{m}\right)=\left(\frac{2}{m}\right)^b(-1)^{\frac{u-1}{2}\frac{m-1}{2}}\left(\frac{m}{|u|}\right).$$

由此定理,可推得

$$\left(\frac{d}{m}\right)=\left(\frac{d}{|d|+m}\right).$$

故有

定理 2. Kronecker 符號 $\left(\frac{d}{m}\right)$ 爲模 $|d|$ 的實特徵.

定理 3. 設 $m>0$, $n>0$, $m\equiv -n \pmod{|d|}$,則

$$\left(\frac{d}{m}\right)=\begin{cases}\left(\frac{d}{n}\right), & 若\ d>0,\\ -\left(\frac{d}{n}\right), & 若\ d<0.\end{cases}$$

證: 因

$$\left(\frac{d}{m}\right)=\left(\frac{d}{n|d|-n}\right)=\left(\frac{d}{n(|d|-1)}\right)=\left(\frac{d}{n}\right)\left(\frac{d}{|d|-1}\right).$$

故當 d 爲奇數時,由定理 1, 得

$$\left(\frac{d}{|d|-1}\right)=\left(\frac{|d|-1}{|d|}\right)=\left(\frac{-1}{|d|}\right)=(-1)^{\frac{|d|-1}{2}}=\begin{cases}1, & 若\ d>0,\\ -1, & 若\ d<0.\end{cases}$$

而當 d 爲偶數時,記 $d=2^b u$, $2\nmid u$, $b\geqslant 2$, 則由定理 1, 得

$$\left(\frac{d}{|d|-1}\right)=\left(\frac{2}{|d|-1}\right)^b(-1)^{\frac{u-1}{2}}\left(\frac{|d|-1}{|u|}\right)=(-1)^{\frac{u-1}{2}}\left(\frac{-1}{|u|}\right)=$$

$$=(-1)^{\frac{u-1}{2}+\frac{|u|-1}{2}}=\begin{cases}1, & 若\ d>0,\\ -1, & 若\ d<0.\end{cases}$$

故得定理.

定理 4. 設 $k>0$, $(d,k)=1$. 同餘式

$$x^2\equiv d \pmod{4k} \tag{1}$$

之解數等於

$$2\sum_{f\mid k}\left(\frac{d}{f}\right).$$

此處 f 過 k 之諸無平方因子之正因子.

顯然,若 x 是一解,則 $x+2k$ 亦然. 故由定理可得

$$x^2\equiv d \pmod{4k}, \qquad 0\leqslant x<2k$$

之解數等於 $\sum_{f|k}\left(\frac{d}{f}\right)$.

證: 1) 若 d 爲奇數,則 $d\equiv 1 \pmod 4$,而 $(d, 4k)=1$. 由定理 3.5.1, 可知同餘式

$$x^2\equiv d \pmod{p^l}$$

之解數爲

$$\begin{cases} 2, & 若\ p=2,\quad l=2, \\ 2\left(1+\left(\frac{d}{p}\right)\right), & 若\ p=2,\quad l>2, \\ 1+\left(\frac{d}{p}\right), & 若\ p>2. \end{cases}$$

由定理 2.8.1, 可知 (1) 式之解數爲

$$2\prod_{p|k}\left(1+\left(\frac{d}{p}\right)\right)=2\sum_{f|k}\left(\frac{d}{f}\right).$$

2) 設 d 爲偶數,則 $d\equiv 0 \pmod 4$. 故 k 是奇數.

$$x^2\equiv d\equiv 0 \pmod 4$$

有二解.

$$x^2\equiv d \pmod{p^l}$$

有 $1+\left(\frac{d}{p}\right)$ 個解. 故由定理 2.8.1, 可知 (1) 式之解數等於

$$2\prod_{p|k}\left(1+\left(\frac{d}{p}\right)\right)=2\sum_{f|k}\left(\frac{d}{f}\right).$$

§4. 二次型表整數之表法數.

定義. 若 $(a, b, c)=1$, 則 $\{a, b, c\}$ 謂之原型. 若 $(a, b, c)=g>1$, 則 $\{a, b, c\}$ 謂之非原型.

顯然 $\left(\frac{a}{g}, \frac{b}{g}, \frac{c}{g}\right)$ 爲原型,其判別式等於 d/g^2. 又若 $\{a, b, c\}\sim\{a_1, b_1, c_1\}$, 則二者同爲原型或非原型.

以 $h(d)$ 表以 d 爲判別式之原型之類數.

顯然以 d 爲判別式之型之類數等於

$$\sum_{\substack{g^2|d\\g>0}} h\left(\frac{d}{g^2}\right).$$

於諸原型類中每類取一代表(若爲定型,則討論諸原定正型類),而得一代表系. 命之爲

$$F_1, \cdots, F_{h(d)}.$$

定理 1. 設 $k>0$, $(k, d)=1$. 命 $\psi(k)$ 表諸等式

$$k=F_1(x, y), \cdots, \quad k=F_{h(d)}(x, y)$$

之原解之個數之總和. 則

$$\psi(k)=w\sum_{n|k}\left(\frac{d}{n}\right).$$

(關於原解及 w 之定義,請參考前章 §4.)

證: 先從同餘式

$$l^2 \equiv d \pmod{4k}, \qquad 0 \leqslant l<2k$$

之解說起. 對此式之一解 l, 由 $l^2-4km=d$ 可定出一整數 m. 如此得一型 $\{k, l, m\}$, 易證 $\{k, l, m\}$ 爲原型, 且有判別式 d. 故 $\{k, l, m\}$ 與 F_i 中之一相似,且恰與一相似. 又由定理 11.4.3 已知對每一 l 有 w 個既約原解. 故

$$k=F_1(x, y), \cdots, \quad k=F_{h(d)}(x, y)$$

之既約原解之總數爲

$$w\sum_{f|k}\left(\frac{d}{f}\right).$$

又諸原解之總數爲

$$\psi(k)=w\sum_{\substack{g^2|k\\g>0}}\sum_{f|\frac{k}{g^2}}\left(\frac{d}{f}\right)$$

$\left(\text{因 } (k, d)=1, \text{ 故 } \left(\frac{k}{g^2}, d\right)=1\right)$. 因 $(g^2, d)=1$, 故

$$\psi(k)=w\sum_{\substack{g^2|k\\g>0}}\sum_{f|\frac{k}{g^2}}\left(\frac{d}{fg^2}\right)=w\sum_{n|k}\left(\frac{d}{n}\right).$$

(因任一整數 n 必可表成 $n=fg^2$, f 無平方因子及 $g>0$. 又 $g^2|k$, $f|\frac{k}{g^2}$,與 $n|k$ 相當,反之亦然.)

今舉本定理之一應用.

易證 $h(-4)=1$, 故 $\psi(k)$ 卽爲 $k=x^2+y^2$ 之解數. 故得:

定理 2. $x^2+y^2=k$ 之解數等於四倍於 k 之因數 $\equiv 1 \pmod 4$ 者之個數減去 k 之因數 $\equiv 3 \pmod 4$ 者之個數.

此與定理 6.7.5 之結果完全相符合.

習題 1. 若 m 爲奇數, $x^2+2y^2=2^l m$ 之解數等於 2σ, 此處 σ 爲 m 之因數 $\equiv 1$ 或 $3 \pmod 8$ 者之個數減去 m 之因數 $\equiv 5$ 或 $7 \pmod 8$ 者之個數.

習題 2. $k=x^2+xy+y^2$ 之解數爲 $6E(k)$. 此 $E(k)$ 爲 k 中形如 $3h+1$ 之因數之個數減去形如 $3h+2$ 之因數之個數.

習題 3. 若 m 爲奇數,則 $x^2+3y^2=2^l m$ 之解數有三種情形: 若 l 是奇數,則無解; 若 $l=0$, 則解數爲 $2E(m)$; 若 l 爲正偶數, 則解數爲 $6E(m)$. 此處 $E(m)$ 之定義如上.

習題 4. 若 m 爲奇數,則 $x^2+3y^2=4m$ 有 $E(m)$ 個正奇數解.

習題 5. 若 m 爲奇數,則 $x^2+4y^2=2^k m$ 之解數,當 $k=0$ 時爲 $2E$, 當 $k=1$ 時爲 0, 當 $k\geqslant 2$ 時爲 $2E$, 此處 E 爲 m 之素因子 $\equiv 1 \pmod 4$ 者之個數減去 k 之因子 $\equiv 3 \pmod 4$ 者之個數.

習題 6. 用 $e(n)$ 記 n 之因子中 $\equiv 1,2,4 \pmod 7$ 者之個數減去 $\equiv 3,5,6 \pmod 7$ 者之個數所得之差,則 $0<n=x^2+xy+2y^2$ 之解數爲 $2e(n)$.

習題 7. 若 m 爲奇數,則 $e(2^a m)=(a+1)e(m)$. 若 $3\nmid t$, 則當 b 爲奇數時, $e(3^b t)=0$, 當 b 爲偶數時, $e(3^b t)=e(t)$.

習題 8. 若 m 爲正奇數, 則 $m=x^2+7y^2$ 之解數爲 $2e(m)$; $2m = = x^2+7y^2$ 之解數爲 0; $4k=x^2+7y^2$ 之解數爲 $2e(k)$, k 爲整數.

習題 9. 若 m 爲正奇數,則 $x^2+7y^2=8m$ 恰有 $e(m)$ 個正整數解.

習題 10. $0<m=x^2+xy+3y^2$ 之解數等於 m 諸因子中 $\equiv 1,3,4,5,9 \pmod{11}$ 者之個數減去 $\equiv 2,6,7,8,10 \pmod{11}$ 者之個數所得之差的二倍.

§5. 二次型的 mod q 相似.

命 q 爲一大於 1 的素數. 若有一整係數變換

$$x=rX+sY, \quad y=tX+uY, \quad (ru-st, q)=1 \tag{1}$$

使

$$ax^2+bxy+cy^2 \equiv a_1X^2+b_1XY+c_1Y^2 \pmod q, \tag{2}$$

則謂二次型 $\{a, b, c\}$ 與 $\{a_1, b_1, c_1\}$ mod q 相似. 命 d, d_1 分別表示 $\{a, b, c\}$ 與 $\{a_1, b_1, c_1\}$ 的判別式,則顯然有

$$d_1 \equiv (ru-st)^2(b^2-4ac) \equiv (ru-st)^2 d \pmod q. \tag{3}$$

由 (3) 式可知若 $\{a, b, c\}$ 與 $\{a_1, b_1, c_1\}$ mod p 相似,則必

$$\left(\frac{d}{p}\right)=\left(\frac{d_1}{p}\right).$$

取 q 爲一大於 2 的奇素數 p. 設型 $\{a, b, c\}$ 的判別式爲 d, 且 $p \nmid d$, 則 $\{a, b, c\}$ 一定與一形如 $\{a_1, 0, c_1\}$ 的型 mod p 相似. 蓋因 $p \nmid (a, b, c)$, 若 $p \nmid a$, 則命 $X \equiv x+\frac{b}{2a}y$, $Y \equiv y \pmod p$, 可得

$$ax^2+bxy+cy^2 \equiv a\left(x+\frac{b}{2a}y\right)^2-\frac{d}{4a}y^2 \equiv aX^2-\frac{d}{4a}Y^2 \pmod p;$$

若 $p \nmid c$, 也可類似地證之;若 $p \mid (a, c)$, 而 $p \nmid b$, 則命 $x=X+Y$, $y=X-Y$, 得

$$ax^2+bxy+cy^2 \equiv bxy \equiv bX^2-bY^2 \pmod p.$$

故對於這種情形,今後不妨假定 $p \mid b$, $p \nmid ac$ 而討論之.

引理 1. 若 $p \nmid ac$, 則必有 x, y 使

$$ax^2+cy^2 \equiv 1 \pmod p.$$

證: 命 x, y 各各經過 $0, 1, \cdots, p-1$, 則 ax^2 與 $1-cy^2$ 各有 $\frac{p+1}{2}$ 個不同的值. 所以必有一組 x, y 使

$$ax^2 \equiv 1-cy^2 \pmod p,$$

亦卽引理.

令 $1 \equiv ar^2+ct^2 \pmod p$, 而命 s, u 爲任何一對適合 $p \nmid ru-st$ 的整數, 固定 s, u 而命

$$b_1 \equiv 2ars+2ctu, \quad c_1 \equiv as^2+cu^2 \pmod p,$$

則必 $\{a, 0, c\} \sim \{1, b_1, c_1\} \pmod p$. 若命 d_1 爲後者的判別式,則由前面的討

論必有

$$\{1, b_1, c_1\} \sim \left\{1, 0, -\frac{d_1}{4}\right\} \sim \{1, 0, -d_1\} \qquad (\bmod p).$$

總結以上所述,可得:

定理 1. 設 $\{a, b, c\}$ 的判別式爲 d, 而 $p > 2$, $p \nmid d$, 又命 r 爲 mod p 的任一二次非剩餘,則當 $\left(\frac{d}{p}\right) = 1$ 時,

$$\{a, b, c\} \sim \{1, 0, -1\} \sim \{0, 1, 0\} \qquad (\bmod p);$$

而當 $\left(\frac{d}{p}\right) = -1$ 時,

$$\{a, b, c\} \sim \{1, 0, -r\} \qquad (\bmod p);$$

又 $\{1, 0, -1\}$ 必不能與 $\{1, 0, -r\}$ mod p 相似.

系. 判別式相同的二次型必互相 mod p 相似, p 爲一不能整除 d 的奇素數.

對於 $q = 2$, 而二次型有奇判別式的情形,有:

定理 2. 任何有奇判別式的二次型,必與下列二型

$$\{0, 1, 0\}, \qquad \{1, 1, 1\}$$

之一 mod 2 相似,且僅與其中之一相似. 具體言之,

$$\{a, b, c\} \sim \{0, 1, 0\} \quad (\bmod 2), \qquad 若\ 2 \mid ac;$$

$$\{a, b, c\} \sim \{1, 1, 1\} \quad (\bmod 2), \qquad 若\ 2 \nmid ac.$$

證: 因 $2 \nmid d$, 故 $2 \nmid b$, 故若 $2 \nmid ac$, 則

$$ax^2 + bxy + cy^2 \equiv x^2 + xy + y^2 \qquad (\bmod 2);$$

若 $2|ac$, 則必 $2|a$ 或 $2|c$. 若 $2|a$, 則

$$ax^2 + bxy + cy^2 \equiv xy + cy^2 \equiv y(x + cy) \qquad (\bmod 2),$$

故得 $\{a, b, c\} \sim \{0, 1, 0\}$ (mod 2); 若 $2|c$, 也可用同法得之.

又 $\{0, 1, 0\}$ 不能與 $\{1, 1, 1\}$ mod 2 相似,故得定理.

系. 任何二個有相同的奇判別式的二次型,必 mod 2 相似.

今考慮 p 能整除二次型的判別式的情形.

引理 2. 命 n 表一已與之整數,則必有二整數 x, y, $(x, y) = 1$, 且使

$$(F(x,y),n)=1.$$

證: 命 q 爲任一素數. 因 $F(x,y)$ 爲一原型, 故 $q\nmid(a,b,c)$. 若 $q\nmid a$, 則 $q\nmid F(1,0)$; 若 $q\nmid c$, 則 $q\nmid F(0,1)$; 若 $q|(a,c)$, 而 $q\nmid b$, 則 $q\nmid F(1,1)$. 故若 $n=q$, 則定理已明.

命 $q_1,\cdots,q_s$ 爲 n 的所有不同的素因子,由以上所述,必有整數 x_i, y_i, 使

$$q_i\nmid F(x_i,y_i).$$

由孫子定理可知有二整數 x, y 使

$$X\equiv x_i \pmod{q_i},\ Y\equiv y_i \pmod{q_i} \qquad (i=1,\cdots,s).$$

顯然可見

$$(F(X,Y),n)=1.$$

又命 $x=X/(X,Y)$, $y=Y/(X,Y)$, 則 $(x,y)=1$. 而

$$(F(x,y),n)=1.$$

先考慮 $p>2$, 而型 $\{a,b,c\}$ 的判別式 d 適合 $p|d$ 的情形. 因 $p\nmid(a,c)$, 故今後不妨假定 $p\nmid a$. 易證

$$\{a,b,c\}\sim\{a,0,0\} \qquad (\bmod p).$$

定理 3. $p>2$, 二次型 $\{a,b,c\}$ 與 $\{a_1,b_1,c_1\}$ 的判別式各爲 d 及 d_1, 且 $p|d$, $p|d_1$. 則 $\{a,b,c\}$ 與 $\{a_1,b_1,c_1\}$ 能 mod p 相似的充分必要條件爲

$$\left(\frac{k}{p}\right)=\left(\frac{k_1}{p}\right),$$

其中 k, k_1 各爲任何能經 $\{a,b,c\}$, $\{a_1,b_1,c_1\}$ 表出且適合 $(k,d)=1$, $(k_1,d)=1$ 的整數.

證: 由引理 2, 可知 k, k_1 之存在. 命 $k\equiv ax^2+bxy+cy^2 \pmod p$, $(k,p)=1$, 則

$$\left(\frac{k}{p}\right)=\left(\frac{ax^2+bxy+cy^2}{p}\right)=\left(\frac{ax_1^2}{p}\right)=\left(\frac{a}{p}\right).$$

所以 $\left(\frac{k}{p}\right)$ 爲一常數,且卽等於 $\left(\frac{a}{p}\right)$. 今若 $\{a,b,c\}$ 與 $\{a_1,b_1,c_1\}$ mod p 相似,則由相似的定義,立得

$$\left(\frac{k}{p}\right)=\left(\frac{a}{p}\right)=\left(\frac{a_1}{p}\right)=\left(\frac{k_1}{p}\right).$$

反之若 $\left(\frac{k}{p}\right)=\left(\frac{k_1}{p}\right)$,則 $\left(\frac{a}{p}\right)=\left(\frac{a_1}{p}\right)$,故有整數 z 使

$$a \equiv a_1 z^2 \qquad (\bmod p).$$

故得

$$\{a, b, c\} \sim \{a, 0, 0\} \sim \{a_1, 0, 0\} \sim \{a_1, b_1, c_1\} \qquad (\bmod p).$$

下面我們來討論 $p=2$, 而 $2|d$ 的情形. 先引進符號:

$$\delta(k)=(-1)^{\frac{k-1}{2}}, \qquad 若\ \frac{d}{4}\equiv 0\ 或\ 3\ (\bmod 4);$$

$$\varepsilon(k)=(-1)^{\frac{k^2-1}{8}}, \qquad 若\ \frac{d}{4}\equiv 0\ 或\ 2\ (\bmod 8);$$

$$\delta(k)\varepsilon(k)=(-1)^{\frac{k-1}{2}+\frac{k^2-1}{8}}, \qquad 若\ \frac{d}{4}\equiv 0\ 或\ 6\ (\bmod 8);$$

其中 k 爲能經 $\{a, b, c\}$ 表出的奇整數.

因 $2|d$, 故必 $2|b$, 故今後不妨假定 $b=0$ 而討論

$$ax^2+cy^2, \qquad d=-4ac.$$

定理 4. 二個適合 $\frac{d}{4}\equiv 3\ (\bmod 4)$ 的二次型 mod 4 相似的充分必要條件爲他們有相同的 δ.

證: 因 $d=-4ac$, 故 $ac\equiv 1\ (\bmod 4)$, 亦卽 $a\equiv c\ (\bmod 4)$. 若 $2\nmid k$, 且 k 能表成

$$k\equiv ax^2+cy^2\equiv a(x^2+y^2) \qquad (\bmod 4),$$

因 x, y 不能同時爲奇或偶,故必 $k\equiv a\ (\bmod 4)$, 所以得到

$$\delta(k)=\delta(a).$$

由此極易推得定理.

用同樣的方法可以證明下列諸定理:

定理 5. 二個適合 $\frac{d}{4}\equiv 2\ (\bmod 8)$ 的二次型 mod 8 相似的充分必要條件爲他們有相同的 ε.

定理 6. 二個適合 $\frac{d}{4}\equiv 6\ (\bmod 8)$ 的二次型 mod 8 相似的充分必要條件爲他們有相同的 $\delta\varepsilon$.

定理 7. 二個適合 $\frac{d}{4}\equiv 0\ (\bmod 4)$ 的二次型 mod 4 相似的充分必要條件

爲他們有相同的 δ.

定理 8. 二個適合 $\frac{d}{4}\equiv 0 \pmod 8$ 的二次型 mod 8 相似的充分必要條件爲他們有相同的 δ 及 ε.

習題 1. 任何二個適合$\frac{d}{4}\equiv 2 \pmod 4$ 的二次型必 mod 4 相似.

習題 2. 任何二個適合$\frac{d}{4}\equiv 1 \pmod 4$ 的二次型必 mod 4 相似.

習題 3. 任何適合 $\frac{d}{4}\equiv 1 \pmod 4$ 的型必與

$$x^2+3y^2, \qquad x^2+7y^2$$

之一 mod 8 相似，且僅與其中之一 mod 8 相似. 並由此推出任何二個具有相同判別式 d, 而$\frac{d}{4}\equiv 1 \pmod 4$ 的二次型,必爲 mod 8 相似.

習題 4. 命 q 爲任一正整數. 任二個二次型對 mod q 相似之必要且充分條件爲其特徵系全同.

§ 6. 二次型的特徵系. 族.

由相似及 mod q 相似的定義,立刻得到若二個二次型相似,則對任何 q, 他們必爲 mod q 相似.

定 義 1. 命 $p_1, \cdots, p_s$ 爲 d 之奇素因子. 若 $(k, 2d)=1$, 且可以 $F(x,y)$ 表出之,則由上節之討論可知

$$\left(\frac{k}{p_i}\right),\ \delta(k),\ \varepsilon(k),\ \delta(k)\varepsilon(k) \tag{1}$$

之值不因 k 而異. 稱他們爲 $F(x, y)$ 的特徵系.

因此二相似的二次型有相同的特徵系,所以可以定義二次型類的特徵系.

定 義 2. 若二個有相同判別式 d 的二次型類的每個特徵値都相等,則稱他們爲屬於同一族.

易見族乃由若干類所組成，今後將證明每一族中所含的類數相等. 因此項事實在研究二次域上理想數時,更爲直覺,故不在此處證明.

族的概念主要是由於討論用二次型表整數的問題所引起.

命 $F(x, y)$ 表一固定的二次原型. 今往討論不定方程式

$$k=F(x, y). \tag{2}$$

若 $h(d)=1$, 則此問題可由定理 4.1 解決之. 但若 $h(d)\neq 1$, 則定理 4.1 僅

給與若干不完整的結果. 例如若 $\psi(k)=0$, 則 (2) 式無解; 但若 $\psi(k)\neq 0$, 則 (2) 式有解否?苟有解,則解數多少?此皆非定理 4.1 之所能回答者. 族的引入,對於這個問題的解決,也有部分幫助.

例 1. $d=-96$, 共有四個定正已化原型

$$\{1,0,24\},\ \{3,0,8\},\ \{4,4,7\},\ \{5,2,5\}.$$

由定理 4.1 僅知如以此四型表 k, 則解數之總和為

$$\psi(k)=2\sum_{n|k}\left(\frac{-6}{n}\right),$$

此處 n 經過 k 的所有的正因子. 為欲算出特徵系, 必先選出與 d 互素之 k, 且可由該型表出者. 今各取

$$k=1,\ 11,\ 7,\ 5,$$

因之算出

型	$\left(\frac{k}{3}\right)$	$\delta(k)$	$\varepsilon(k)$
$\{1,0,24\}$	$+1$	$+1$	$+1$
$\{3,0,8\}$	-1	-1	-1
$\{4,4,7\}$	$+1$	-1	$+1$
$\{5,2,5\}$	-1	$+1$	-1

此表完全說明每族包有一類. 由此得出: 當 $k\equiv 1,11,7,5 \pmod{12}$ 時, $\psi(k)$ 各表了第一, 第二, 第三, 第四型之解數. 更具體些, 若 $k\equiv 1 \pmod{12}$, 則 $\psi(k)=2\sum_{n|k}\left(\frac{-6}{n}\right)$ 表

$$x^2+24y^2=k$$

的解數. 同時,也已證明當 $k\equiv 11,7,5 \pmod{12}$ 時,上式不可解.

例 2. $d=-15$. 共有兩個定正已化原型:

$$\{1,1,4\},\quad \{2,1,2\}.$$

各取 $k=1$ 及 17, 各得

$$\left(\frac{k}{3}\right)=\left(\frac{k}{5}\right)=1,$$

及

$$\left(\frac{k}{3}\right)=\left(\frac{k}{5}\right)=-1.$$

由此二者可以算出 $k\equiv 1,4 \pmod{15}$ 及 $k\equiv 2,8 \pmod{15}$. 即得若 $k\equiv 7$, 11,13 或 14 $\pmod{15}$, 則 k 不能以此二型之任一表之. 而 $k\equiv 1,4 \pmod{15}$, 則 $\{1,1,4\}$ 表 k 之方法數等於 $2\sum_{n|k}\left(\frac{-15}{n}\right)$; 若 $k\equiv 2,8 \pmod{15}$, 則 $\{2,1,2\}$ 表 k 之方法數也如此.

由上面二例可以看到, 若每族中祇含有一類, 則當 $(k, 2d)=1$ 時, (2) 的解數可以完全確定.

茲將 $d>-400$ 之每族祇有一類之情況列表如下 (351 頁). 表中還列出所有的定正已化原型.

習題: 如例題, 研究 $d=-20, -24, -32, -35, -51, -75$ 時之情況.

§ 7. 級數 $K(d)$ 之收斂性.

命

$$K(d)=\sum_{n=1}^{\infty}\left(\frac{d}{n}\right)\frac{1}{n}. \tag{1}$$

此乃一非常重要之級數.

因 $\left(\frac{d}{n}\right)$ 為模 $|d|$ 之實特徵, 故由定理 7.2.3 可得

$$\left|\sum_{a\leqslant n\leqslant b}\left(\frac{d}{n}\right)\right|<|d|.$$

再由定理 6.9.2, 可知級數 $K(d)$ 收斂.

定理 1.

$$\lim_{\tau\to\infty}\frac{1}{\tau}\sum_{\substack{1\leqslant k\leqslant\tau\\(k,d)=1}}\sum_{n|k}\left(\frac{d}{n}\right)=\frac{\varphi(|d|)}{|d|}K(d).$$

證: 1) 命 $A(\tau; d, n)$ 表示不大於 $\frac{\tau}{n}$ 而與 d 互素之整數之個數, 則

$$\frac{1}{\tau}\sum_{\substack{1\leqslant k\leqslant\tau\\(k,d)=1}}\sum_{n|k}\left(\frac{d}{n}\right)=\frac{1}{\tau}\sum_{n=1}^{\infty}\left(\frac{d}{n}\right)\sum_{\substack{1\leqslant k\leqslant\tau\\(k,d)=1\\n|k}}1=\frac{1}{\tau}\sum_{n=1}^{\infty}\left(\frac{d}{n}\right)\sum_{\substack{1\leqslant k\leqslant\tau/n\\(k,d)=1}}1=$$

$$=\sum_{n=1}^{\infty}\left(\frac{d}{n}\right)\frac{A(\tau; d, n)}{\tau}. \tag{2}$$

$-d=3$	1,1,1
4	1,0,1
7	1,1,2
8	1,0,2
11	1,1,3
12	1,0,3
15	1,1,4
	2,1,2
16	1,0,4
19	1,1,5
20	1,0,5
	2,2,3
24	1,0,6
	2,0,3
27	1,1,7
28	1,0,7
32	1,0,8
	3,2,3
35	1,1,9
	3,1,3
36	1,0,9
	2,2,5
40	1,0,10
	2,0,5
43	1,1,11
48	1,0,12
	3,0,4
51	1,1,13
	3,3,5
52	1,0,13
	2,2,7
60	1,0,15
	3,0,5
64	1,0,16
	4,4,5
67	1,1,17
72	1,0,18
	2,0,9
75	1,1,19
	3,3,7
84	1,0,21
	2,2,11
	3,0,7
	5,4,5
88	1,0,22
	2,0,11
91	1,1,23
	5,3,5

$-d=96$	1,0,24
	3,0,8
	4,4,7
	5,2,5
99	1,1,25
	5,1,5
100	1,0,25
	2,2,13
112	1,0,28
	4,0,7
115	1,1,29
	5,5,7
120	1,0,30
	2,0,15
	3,0,10
	5,0,6
123	1,1,31
	3,3,11
132	1,0,33
	2,2,17
	3,0,11
	6,6,7
147	1,1,37
	3,3,13
148	1,0,37
	2,2,19
160	1,0,40
	4,4,11
	5,0,8
	7,6,7
163	1,1,41
168	1,0,42
	2,0,21
	3,0,14
	6,0,7
180	1,0,45
	2,2,23
	5,0,9
	7,4,7
187	1,1,47
	7,3,7
192	1,0,48
	3,0,16
	4,4,13
	7,2,7

$-d=195$	1,1,49
	3,3,17
	5,5,11
	7,1,7
228	1,0,57
	2,2,29
	3,0,19
	6,6,11
232	1,0,58
	2,0,29
235	1,1,59
	5,5,13
240	1,0,60
	3,0,20
	4,0,15
	5,0,12
267	1,1,67
	3,3,23
280	1,0,70
	2,0,35
	5,0,14
	7,0,10
288	1,0,72
	4,4,19
	8,0,9
	8,8,11
312	1,0,78
	2,0,39
	3,0,26
	6,0,13
315	1,1,79
	5,5,17
	7,7,13
	9,9,11
340	1,0,85
	2,2,43
	5,0,17
	10,10,11
352	1,0,88
	4,4,23
	8,0,11
	8,8,13
372	1,0,93
	2,2,47
	3,0,31
	6,6,17

因當 n 增大時，$A(\tau; d, n)$ 決不增加；又因

$$\frac{A(\tau; d, n)}{\tau} \leqslant \frac{1}{n},$$

故由定理 6.8.2，可知級數 (2) 關於 τ 為一致收斂.

又對固定之 n 有

$$\lim_{\tau\to\infty} \frac{A(\tau; d, n)}{\tau} = \frac{\varphi(|d|)}{|d|} \frac{1}{n}.$$

故得

$$\lim_{\tau\to\infty} \frac{1}{\tau} \sum_{\substack{1\leqslant k\leqslant\tau \\ (k,d)=1}} \sum_{n|k} \left(\frac{d}{n}\right) = \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) \lim_{\tau\to\infty} \frac{A(\tau; d, n)}{\tau} =$$

$$\frac{\varphi(|d|)}{|d|} \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) \frac{1}{n}.$$

§8. 雙曲扇形及橢圓內之整點數.

定理 1. 設 $m>0$，與一以原點為中心之橢圓或一以原點為中心之雙曲扇形（由雙曲線之弧及由原點出發之二射線所構成）. 命 I 為其面積（有限的）. 將原圖形放大 $\sqrt{\tau}$ 倍（即以 $\xi\sqrt{\tau}$, $\eta\sqrt{\tau}$ 代 ξ, η）. 命 $U(\tau)$ 表此放大的圖形中之整點，其坐標皆適合

$$\xi \equiv \xi_0 \pmod m, \qquad \eta \equiv \eta_0 \pmod m$$

者之個數，則

$$\lim_{\tau\to\infty} \frac{U(\tau)}{\tau} = \frac{I}{m^2}.$$

證： 在原圖形之平面上作網. 以

$$\xi = \frac{\xi_0 + rm}{\sqrt{\tau}}, \qquad \eta = \frac{\eta_0 + sm}{\sqrt{\tau}}$$

為其經緯. 網眼為邊長 $\frac{m}{\sqrt{\tau}}$ 之正方形.

命 $W(\tau)$ 為網眼之“西南角”在橢圓或雙曲扇形中者之個數. 則顯然有

$$U(\tau) = W(\tau).$$

今網眼之面積為 $\frac{m^2}{\tau}$，由積分之基本定理立得

$$I = \iint d\xi\, d\eta = \lim_{\tau\to\infty} \frac{m^2}{\tau} W(\tau).$$

故得定理。

§ 9. **平均極限.**

命 $\psi(k,F)$ 表用 F 表 k 之原表示之個數,又命

$$H(\tau,F)=\sum_{\substack{1\leqslant k\leqslant\tau\\(k,d)=1}}\psi(k,F),\qquad \tau>1.$$

本節之目的在求出極限

$$\lim_{\tau\to\infty}\frac{1}{\tau}H(\tau,F).$$

定理 1. 當 x,y 各過完全剩餘系 mod $|d|$ 時,恰有 $|d|\,\varphi(|d|)$ 組值使 $F(x,y)$ 與 d 互素.

證: 祇須證明: 若 $p^l|d$, $l>0$, 則 x,y 於模 p^l 之完全剩餘系中恰有 $p^l\varphi(p^l)$ 組使 $p\nmid F(x,y)$ 卽可. 蓋命 $|d|$ 之標準分解式爲 $\prod_i p_i^{l_i}$, 則因 $(d,F(x,y))=1$ 與 $p\nmid F(x,y)$ 等價,故由孫子定理可知當 x,y 各過模 $|d|$ 之完全剩餘系時,共有

$$\prod_{p\,|\,|d|}p^l\varphi(p^l)=|d|\,\varphi(d)$$

個值使 $F(x,y)$ 與 d 互素.

因 $(a,b,c)=1$, 故 $p\nmid(a,c)$. 今設 $p\nmid a$.

1) 設 $p>2$. 因 $(p,4a)=1$, 故由

$$4aF=(2ax+by)^2-dy^2\not\equiv 0\qquad(\bmod p),$$

可知

$$2ax+by\not\equiv 0\qquad(\bmod p).$$

且反之亦然. 對 y 之任一值 (共有 p^l 個值),因 $p\nmid 2a$, 故 x 有 $p-1$ 個不同值, mod p. 卽 x 有 $p^{l-1}(p-1)=\varphi(p^l)$ 個值 mod p^l. 故得定理.

2) 設 $p=2$. 由 $2|d$ 可知 $2|b$. 條件

$$ax^2+bxy+cy^2\equiv 1\qquad(\bmod 2),$$

卽爲

$$ax+cy\equiv 1\qquad(\bmod 2).$$

因對 y 之任一值 (共有 2^l 個) 有 2^{l-1} 個 x 之值 (mod 2^l) 使上式成立,故得

定理.

定理 2. 吾人有

$$\lim_{\tau\to\infty}\frac{\bar{H}(\tau,F)}{\tau}=\begin{cases}\dfrac{2\pi}{\sqrt{|d|}}\ \dfrac{\varphi(|d|)}{|d|}, & \text{若}\ d<0,\\[2mm] \dfrac{\log\varepsilon}{\sqrt{d}}\ \dfrac{\varphi(d)}{d}\ , & \text{若}\ d>0.\end{cases}$$

證: 若 $d<0$, 命 $U(\tau)=U(\tau,F,x_0,y_0)$ 表示適合

$$0\leqslant F(x,y)\leqslant\tau,$$

$$x\equiv x_0\pmod{|d|},\qquad y\equiv y_0\pmod{|d|}$$

之解數. 若 $d>0$, 則命 $U(\tau)=U(\tau,F,x_0,y_0)$ 表示適合

$$0\leqslant F(x,y)\leqslant\tau,\quad \bar{L}>0,\quad 1\leqslant\left|\frac{L}{\bar{L}}\right|<\varepsilon^2,$$

$$x\equiv x_0\pmod{|d|},\qquad y\equiv y_0\pmod{|d|}$$

之解數. 此處 $L,\bar{L},\varepsilon$ 之定義一如 §11.4.

命 x_0,y_0 各各經過模 $|d|$ 之完全剩餘系中使 $(F(x_0,y_0),d)=1$ 之整數組, 則

$$\sum_{\substack{(x_0,y_0)\\(F(x_0,y_0),d)=1}}U(\tau)=\sum_{\substack{1\leqslant k\leqslant\tau\\(k,d)=1}}\psi(k,F)=H(\tau,F),$$

故有

$$\lim_{\tau\to\infty}\frac{H(\tau,F)}{\tau}=\lim_{\tau\to\infty}\frac{1}{\tau}\sum_{\substack{(x_0,y_0)\\(F(x_0,y_0),d)=1}}U(\tau).$$

由定理 1, 若能證明對每一組 x_0,y_0, 均有

$$\lim_{\tau\to\infty}\frac{U(\tau)}{\tau}=\begin{cases}\dfrac{2\pi}{\sqrt{|d|}}\ \dfrac{1}{d^2}, & \text{若}\ d<0,\\[2mm] \dfrac{\log\varepsilon}{\sqrt{d}}\ \dfrac{1}{d^2}. & \text{若}\ d>0,\end{cases}$$

則定理已得. 再由定理 8.1, 可知祇須求出橢圓 $F(x,y)\leqslant 1$ $(d<0)$ 及雙曲扇形 $0\leqslant F(x,y)\leqslant 1$, $\bar{L}>0$, $1\leqslant\left|\frac{L}{\bar{L}}\right|<\varepsilon^2$ $(d>0)$ 之面積便已足够.

1) 設 $d<0$, 熟知橢圓

$$ax^2 + bxy + cy^2 \leqslant 1$$

之面積為$\frac{2\pi}{\sqrt{|d|}}$，故得定理.

2) 設 $d > 0$, 不妨假定 $a > 0$. 因

$$L = 2ax + (b+\sqrt{d})\,y, \quad \bar{L} = 2ax + (b-\sqrt{d})\,y,$$

故有

$$L\bar{L} = 4a\,(ax^2+bxy+cy^2),$$

而得 $L > 0$.

所求雙曲扇形之面積為

$$I = \iint dx\,dy,$$

其中積分變數過 $L\bar{L} \leqslant 4a$, $\bar{L} > 0$, $1 \leqslant \frac{L}{\bar{L}} < \varepsilon^2$. 換變數

$$\frac{L}{2\sqrt{a}} = \rho, \qquad \frac{\bar{L}}{2\sqrt{a}} = \sigma.$$

此變換之函數行列式 (Jacobian) 之值等於

$$\begin{vmatrix} \frac{\partial\rho}{\partial x} & \frac{\partial\rho}{\partial y} \\ \frac{\partial\sigma}{\partial x} & \frac{\partial\sigma}{\partial y} \end{vmatrix} = \frac{1}{2\sqrt{a}}\;\frac{1}{2\sqrt{a}} \begin{vmatrix} 2a & b+\sqrt{d} \\ 2a & b-\sqrt{d} \end{vmatrix} = -\sqrt{d}.$$

故

$$I = \frac{1}{\sqrt{d}} \iint d\rho\,d\sigma,$$

積分變數過 $\rho\sigma \leqslant 1$, $\sigma > 0$, $\sigma \leqslant \rho < \varepsilon^2\sigma$. 此乃一以 $(0, 0)$, $\left(\varepsilon, \frac{1}{\varepsilon}\right)$, $(1, 1)$ 為頂點之等腰雙曲扇形. 故

$$\begin{aligned} \sqrt{d}\; I &= \int_0^1 d\rho \int_{\rho/\varepsilon^2}^{\rho} d\sigma + \int_1^{\varepsilon} d\rho \int_{\rho/\varepsilon^2}^{1/\rho} d\sigma = \\ &= \int_0^1 \left(\rho - \frac{\rho}{\varepsilon^2}\right) d\rho + \int_1^{\varepsilon} \left(\frac{1}{\rho} - \frac{\rho}{\varepsilon^2}\right) d\rho = \\ &= \int_0^1 \rho\,d\rho + \int_1^{\varepsilon} \frac{d\rho}{\rho} - \int_0^{\varepsilon} \frac{\rho}{\varepsilon^2}\,d\rho = \log\varepsilon. \end{aligned}$$

所以

$$I = \frac{\log\varepsilon}{\sqrt{d}},$$

而得定理.

§10. 類數之解析表示法.

定理 1.

$$h(d)=\begin{cases}\dfrac{w\sqrt{|d|}}{2\pi}K(d), & 若\quad d<0,\\[2ex] \dfrac{\sqrt{d}}{\log\varepsilon}\quad K(d), & 若\quad d>0.\end{cases}$$

證: 命

$$F_1,\cdots,\quad F_{h(d)}$$

爲代表系. 由定理 4.1 可知

$$\sum_F H(\tau,F)=\sum_{\substack{1\leqslant k\leqslant\tau\\(k,d)=1}}\sum_F\psi(k,F)=$$

$$=\sum_{\substack{1\leqslant k\leqslant\tau\\(k,d)=1}}\psi(k)=w\sum_{\substack{1\leqslant k\leqslant\tau\\(k,d)=1}}\sum_{n|k}\left(\frac{d}{n}\right).$$

由定理 7.1 及定理 9.2 可知

$$h(d)\left\{\begin{matrix}2\pi\\ \log\varepsilon\end{matrix}\right\}\frac{\varphi(|d|)}{|d|^{3/2}}=w\frac{\varphi(|d|)}{|d|}K(d)\left\{\begin{matrix}若\quad d<0,\\ 若\quad d>0,\end{matrix}\right.$$

卽得所求.

故今之問題一變而爲求

$$K(d)=\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{d}{n}\right)$$

之和之問題矣.

§11. 基本判別式.

定義. 基本判別式 d 者乃判別式之不含奇素數之平方因子,且 d 或爲奇數或 $\equiv 8 \pmod{16}$ 或 $\equiv 12 \pmod{16}$ 者.

例如: 5, 8, 12, 13, 17, 21, 24, 28, 29, ⋯ .

定理 1. 任一判別式 d 皆可表爲 fm^2 之形式,此處 f 是基本判別式. 且表法是唯一的.

證: 1) 若 d 是奇數, 命 m^2 爲最大之平方數可除盡 d 者. 命 $d=fm^2$, 卽得所求.

2) 若 d 是偶數,先表 $d=qr^2$, r^2 是 d 中之最大平方因子. 顯然有 $2|r$. 若 $q\equiv 1 \pmod 4$, 則 q 卽爲基本判別式

若 $q\equiv 2$ 或 $3 \pmod 4$, 則取 $f=4q$, 如此則 $4q\equiv 8$ 或 $12 \pmod{16}$ 此乃基本判別式.

3) 唯一性.

命 $d=fm^2$, $m>0$, f 爲基本判別式. 若 f 是奇數,則 f 無平方因子,卽 m^2 乃 d 之最大平方因子. 若 f 是偶數.則 $f\equiv 8$ 或 $12 \pmod{16}$,卽 $4\nmid \frac{f}{4}$, 故 $(2m)^2$ 爲 f 之最大平方因子. 由此種說法,唯一性已明.

定理 2. 命 $d=fm^2$ 爲定理 1 中之表示法,則

$$K(d)=\prod_{p|m}\left(1-\left(\frac{f}{p}\right)\frac{1}{p}\right)K(f).$$

證: 吾人有

$$K(d)=\sum_{n=1}^{\infty}\left(\frac{d}{n}\right)\frac{1}{n}=\sum_{n=1}^{\infty}\left(\frac{m^2f}{n}\right)\frac{1}{n}=$$

$$=\sum_{\substack{n=1\\(m,n)=1}}^{\infty}\left(\frac{f}{n}\right)\frac{1}{n}.$$

設 m 之標準分解式爲 $p_1^{l_1}\cdots p_s^{l_s}$, 則由定理 1.7.1, 可知

$$K(d)=K(f)-\sum_{p_i|m}\left(\frac{f}{p_i}\right)\frac{1}{p_i}K(f)+$$

$$+\sum_{\substack{p_i|m,p_j|m\\p_i\neq p_j}}\left(\frac{f}{p_ip_j}\right)\frac{1}{p_ip_j}K(f)-+\cdots=$$

$$=\prod_{p|m}\left(1-\left(\frac{f}{p}\right)\frac{1}{p}\right)K(f).$$

由此可知今後祇須求出 $K(f)$ 之值卽足.

習題. 試證若 d 爲基本判別式,則 $\left(\frac{d}{n}\right)$ 爲一模 $|d|$ 的實原特徵.

§ 12. 類數公式.

今設 d 爲基本判別式. 命

$$\sqrt{\xi}=\begin{cases}+\sqrt{\xi}, & \text{若 } \xi \text{ 是正數},\\ i\sqrt{|\xi|}, & \text{若 } \xi \text{ 是負數}.\end{cases}$$

定理 1. 若 $0<\varphi<2\pi$, 則

$$\sum_{n=1}^{\infty}\frac{\sin n\varphi}{n}=\frac{\pi}{2}-\frac{\varphi}{2},$$

及

$$\sum_{n=1}^{\infty}\frac{\cos n\varphi}{n}=-\log\left(2\sin\frac{\varphi}{2}\right).$$

證: 由假定, $0<\varphi<2\pi$, 故*

$$\sum_{n=1}^{\infty}\frac{e^{in\varphi}}{n}=-\log(1-e^{i\varphi})=$$

$$=-\log\left(2\sin\frac{\varphi}{2}\right)+i\arctan\left(\cot\frac{\varphi}{2}\right)=$$

$$=-\log\left(2\sin\frac{\varphi}{2}\right)+i\left(\frac{\pi}{2}-\frac{\varphi}{2}\right).$$

將等式兩邊各取實部分和虛部分,即得定理.

定理 2. 若 d 爲基本判別式,則

$$K(d)=\begin{cases}-\dfrac{1}{\sqrt{d}}\displaystyle\sum_{r=1}^{d-1}\left(\frac{d}{r}\right)\log\sin\frac{\pi r}{d}, & 若\quad d>0,\\ -\dfrac{\pi}{|d|^{3/2}}\displaystyle\sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)r, & 若\quad d<0.\end{cases}$$

證: 由特徵和已知

$$\sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)e^{2\pi inr/|d|}=\left(\frac{d}{n}\right)\sqrt{d}.$$

(若 d 爲基本判別式,則$\left(\frac{d}{r}\right)$ 爲原特徵). 故

$$\sqrt{d}\,K(d)=\sum_{n=1}^{\infty}\left(\frac{d}{n}\right)\frac{\sqrt{d}}{n}=\sum_{n=1}^{\infty}\frac{1}{n}\sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)e^{\frac{2\pi i}{|d|}nr}=$$

$$=\sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)\sum_{n=1}^{\infty}\frac{1}{n}e^{\frac{2\pi i}{|d|}nr}.$$

1) 若 $d>0$, 則取上式之實數部分可知

---

*此式之嚴格證明需要用及 Abel 定理. 定理 1 亦可直接證明,讀者可參考熊慶來著,高等算學分析第 501 頁.

$$\sqrt{d}\,K(d)=\sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)\sum_{n=1}^{\infty}\frac{1}{n}\cos\frac{2\pi nr}{d}=$$

$$=-\sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)\log\left(2\sin\frac{\pi r}{d}\right)=$$

$$=-\sum_{r=1}^{d-1}\left(\frac{d}{r}\right)\log\sin\frac{\pi r}{d}$$

（由於 $\log 2\sum_{r=1}^{d-1}\left(\frac{d}{r}\right)=0$）.

2) 若 $d<0$, 則取虛數部分

$$\sqrt{|d|}\,K(d)=\sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)\sum_{n=1}^{\infty}\frac{1}{n}\sin\frac{2\pi rn}{|d|}=$$

$$=\sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)\left(\frac{\pi}{2}-\frac{\pi r}{|d|}\right)=$$

$$=-\frac{\pi}{|d|}\sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)r.$$

由定理 2 及定理 10.1 立得:

定理 3. 設 d 爲基本判別式,則當 $d>0$ 時

$$\varepsilon^{h(d)}=\prod_{t}\sin\frac{\pi t}{d}\Big/\prod_{s}\sin\frac{\pi s}{d};$$

又當 $d<0$ 時

$$h(d)=\frac{w}{2|d|}\left(\sum_{t}t-\sum_{s}s\right),$$

此處 s 過適合 $\left(\frac{d}{r}\right)=1$ 之諸 $r(0<r<|d|)$, 而 t 過適合 $\left(\frac{d}{r}\right)=-1$ 之諸 r.

定理 4. 設 d 爲一負基本判別式,則

$$h(d)=\frac{w}{2\left(2-\left(\frac{d}{2}\right)\right)}\sum_{r=1}^{\left[\frac{|d|}{2}\right]}\left(\frac{d}{r}\right).$$

證: 由定理 1 已知: 當 $2\pi<\varphi<4\pi$ 時,

$$\sum_{n=1}^{\infty}\frac{\sin n\varphi}{n}=\sum_{n=1}^{\infty}\frac{\sin n(\varphi-2\pi)}{n}=\frac{\pi}{2}-\left(\frac{\varphi-2\pi}{2}\right)=\frac{\pi}{2}-\frac{\varphi}{2}+\pi.$$

如定理 2 之證明

$$\sqrt{d}\,K(d)\left(\frac{d}{2}\right)=\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{d}{2n}\right)\sqrt{d}=$$

$$=\sum_{n=1}^{\infty}\frac{1}{n}\sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)e^{\frac{2\pi i}{|d|}\cdot 2nr}.$$

比較虛數部分

$$\sqrt{|d|}\,K(d)\left(\frac{d}{2}\right)=\sum_{n=1}^{\infty}\frac{1}{n}\sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)\sin\frac{4\pi nr}{|d|}=$$

$$=\sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)\sum_{n=1}^{\infty}\frac{1}{n}\sin\frac{4\pi nr}{|d|}=$$

$$=\sum_{1\leqslant r\leqslant\frac{1}{2}|d|}\left(\frac{d}{r}\right)\left(\frac{\pi}{2}-\frac{2\pi r}{|d|}\right)+\sum_{\frac{1}{2}|d|<r\leqslant|d|}\left(\frac{d}{r}\right)\left(\frac{\pi}{2}-\frac{2\pi r}{|d|}+\pi\right).$$

(注意：當 $r=\frac{1}{2}|d|$ 時，該無窮級數之值為 0，而非 $-\frac{\pi}{2}$. 但其時 $\left(\frac{d}{r}\right)=0$，固無害也.) 故

$$\sqrt{|d|}\,K(d)\left(\frac{d}{2}\right)=-\frac{2\pi}{|d|}\sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)r+\pi\sum_{\frac{1}{2}|d|<r<|d|}\left(\frac{d}{r}\right)=$$

$$=2\sqrt{|d|}\,K(d)+\pi\sum_{\frac{1}{2}|d|<r<|d|}\left(\frac{d}{r}\right)=$$

$$=2\sqrt{|d|}\,K(d)-\pi\sum_{1\leqslant r\leqslant\frac{1}{2}|d|}\left(\frac{d}{r}\right),$$

即

$$\sqrt{|d|}\left(2-\left(\frac{d}{2}\right)\right)K(d)=\pi\sum_{1\leqslant r\leqslant\frac{1}{2}|d|}\left(\frac{d}{r}\right).$$

故得定理所云.

習題 1. 試用上二定理中所用之方法，以直接證明

$$|d|\sum_{r=1}^{[\frac{1}{2}|d|]}\left(\frac{d}{r}\right)=\left(2-\left(\frac{d}{2}\right)\right)\sum_{r=1}^{|d|}\left(\frac{d}{r}\right)r.$$

習題 2. 設 $p\equiv 3 \pmod 4$，則於 $0, \frac{1}{2}p$ 之間二次剩餘之個數多於非二次剩餘之個數，若 $p\equiv 1 \pmod 4$，則其數相等.

§ 13. Pell 氏方程的最小解.

今申述以上結果之一應用. 命 $d>1$, 且 $d\equiv 0$ 或 $1 \pmod 4$. 又命 x_0, y_0 爲

$$x^2-dy^2=4$$

之解,使 $x_0+\sqrt{d}\,y_0$ 最小者 ($x_0>0$, $y_0>0$), 而命

$$\varepsilon=\frac{x_0+\sqrt{d}\,y_0}{2}.$$

本節之目的在於證明

$$\varepsilon<d^{\sqrt{d}}.$$

命 $d=m^2f$, 此處 f 爲基本判別式.

定理 1. 命 $f>0$, A^* 爲最小之非負整數 $\equiv A \pmod f$ 者,則

$$\frac{1}{A^*+1}\left|\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{f}{n}\right)\right|\leqslant\frac{1}{2}\left(\sqrt{f}-\frac{A^*+1}{\sqrt{f}}\right).$$

證: 由定理 3.3 可以證明

$$\sum_{a=1}^{f}\sum_{n=1}^{a}\left(\frac{f}{n}\right)=0,$$

故

$$\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{f}{n}\right)=\sum_{a=1}^{A^*}\sum_{n=1}^{a}\left(\frac{f}{n}\right).$$

又可用與定理 7.9.2 相同的方法證明

$$\frac{1}{A^*+1}\left|\sum_{a=1}^{A^*}\sum_{n=1}^{f}\left(\frac{f}{n}\right)\right|\leqslant\frac{1}{2}\left(\sqrt{f}-\frac{A^*+1}{\sqrt{f}}\right),$$

而得定理.

定理 2. 命 $d>1$, 則

$$\left|\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{d}{n}\right)\right|\leqslant A\sqrt{d}.$$

證: 由直接計算可知

$$\left(\frac{d}{n}\right)=\left(\frac{m}{n}\right)^2\left(\frac{f}{n}\right)=\begin{cases}\left(\frac{f}{n}\right), & 若\ (m,n)=1,\\ 0, & 若\ (m,n)>1.\end{cases}$$

故

$$\left|\sum_{a=1}^{A}\sum_{n=1}^{a}\left(\frac{d}{n}\right)\right|=\left|\sum_{a=1}^{A}\sum_{\substack{n=1\\(n,m)=1}}^{a}\left(\frac{f}{n}\right)\right|=$$

$$=\left|\sum_{a=1}^{A}\left(\sum_{n=1}^{a}\left(\frac{f}{n}\right)-\sum_{p|m}\left(\frac{f}{p}\right)\sum_{n=1}^{\left[\frac{a}{p}\right]}\left(\frac{f}{n}\right)+\sum_{\substack{p_1p_2|m\\p_1\neq p_2}}\left(\frac{f}{p_1p_2}\right)\sum_{n=1}^{\left[\frac{a}{p_1p_2}\right]}\left(\frac{f}{n}\right)-\cdots\right)\right|\leqslant$$

$$\leqslant\sum_{k|m}\left|\sum_{a=1}^{A}\sum_{n=1}^{\left[\frac{a}{k}\right]}\left(\frac{f}{n}\right)\right|\leqslant\sum_{k|m}\left\{k\left|\sum_{b=1}^{\left[\frac{A}{k}\right]-1}\sum_{n=1}^{b}\left(\frac{f}{n}\right)\right|+k\left|\sum_{n=1}^{\left[\frac{A}{k}\right]}\left(\frac{f}{n}\right)\right|\right\}\leqslant$$

$$\leqslant\sum_{k|m}k\left\{\frac{1}{2}\left[\frac{A}{k}\right]\sqrt{f}+\left[\frac{A}{k}\right]\right\}\leqslant A\sum_{k|m}\left(\frac{1}{2}\sqrt{f}+1\right)\leqslant$$

$$\leqslant A\sqrt{f}\,m=A\sqrt{d}\,.$$

(因為 $f\geqslant 5$, 故 $1<\frac{1}{2}\sqrt{f}$. 又 $\sum_{k|m}1\leqslant m.$)

定理 3. 命 $d\geqslant 5$, 則

$$K(d)<\frac{1}{2}\log d+1.$$

證: 當 $n\geqslant 1$ 時,命

$$S(n)=\sum_{a=1}^{n}\sum_{k=1}^{a}\left(\frac{d}{k}\right),$$

並定義 $S(-1)=S(0)=0$. 於是有

$$S(n)-S(n-1)=\sum_{k=1}^{n}\left(\frac{d}{k}\right),$$

$$S(n)-2S(n-1)+S(n-2)=\left(\frac{d}{n}\right),\qquad n\geqslant 1.$$

故

$$K(d)=\sum_{n=1}^{\infty}\left(\frac{d}{n}\right)\frac{1}{n}=\sum_{n=1}^{\infty}\frac{1}{n}\{S(n)-2S(n-1)+S(n-2)\}=$$

$$=\sum_{n=1}^{\infty}S(n)\left\{\frac{1}{n}-\frac{2}{n+1}+\frac{1}{n+2}\right\}=$$

$$=\sum_{n=1}^{\infty}\frac{2S(n)}{n(n+1)(n+2)}.$$

命

$$S_1=\sum_{n=1}^{A-1}\frac{2S(n)}{n(n+1)(n+2)},\quad S_2=\sum_{n=A}^{\infty}\frac{2S(n)}{n(n+1)(n+2)}.$$

由於 $|S(n)|\leqslant\frac{n(n+1)}{2}$,故得

$$|S_1|\leqslant\sum_{n=1}^{A-1}\frac{1}{n+2}=\sum_{n=1}^{A-1}\frac{1}{n}-\frac{3}{2}+\frac{1}{A}+\frac{1}{A+1}\leqslant$$

$$\leqslant\log(A-1)+\gamma-\frac{3}{2}+\frac{1}{A}+\frac{1}{A+1}^{*}.$$

又由定理 2，得

$$|S_2|\leqslant\sum_{n=A}^{\infty}\frac{2\sqrt{d}}{(n+1)(n+2)}=\frac{2\sqrt{d}}{A+1}.$$

取 $A=[2\sqrt{d}]+1$，則

$$|K(d)|\leqslant|S_1|+|S_2|\leqslant\log(A-1)+\gamma-\frac{3}{2}+\frac{1}{A}+\frac{2\sqrt{d}+1}{A+1}<\frac{1}{2}\log d+1,$$

(因爲 $d\geqslant5$).

定理 4. 常有

$$\log\varepsilon<\sqrt{d}\left(\frac{1}{2}\log d+1\right).$$

證: 由定理 10.1

$$1\leqslant h(d)=\frac{\sqrt{d}}{\log\varepsilon}K(d).$$

再由定理 3，卽得定理.

定理 5. (Schur). 常有

$$\log\varepsilon<\sqrt{d}\log d.$$

證: 若 $d>e^2$，則由上定理,已得. 若 $d<e^2$，則 $d=5$，但此時

$$\varepsilon=\frac{3+\sqrt{5}}{2},$$

而

---

* $\gamma=0.5772\cdots$ 爲 Euler 常數. $\sum_{n=1}^{x}\frac{1}{n}\leqslant\log x+\gamma$ 之證明可由 $\lim_{x\to\infty}\left(\sum_{n=1}^{x}\frac{1}{n}-\log x\right)=\gamma$ 及 $\sum_{n=1}^{x}\frac{1}{n}-\log x$ 爲一遞增函數而得.

$$\log \varepsilon < \sqrt{5} \log 5,$$

定理成立.

附記: Gauss 曾推測: 當 $|d| \to \infty$ 時,

$$h(d) \to \infty .$$

此乃一著明的難題. 1934 年 Heilbronn 證明,當 $d \to -\infty$ 時,則 $h(d) \to \infty$. 後一年, Siegel 證明

$$\lim_{d \to -\infty} \frac{\log h(d)}{\log |d|} = \frac{1}{2},$$

卽已得出 $h(d)$ 當 $d \to -\infty$ 時之無窮大之主階.

但是否當 $d \to \infty$ 時, $h(d) \to \infty$. 此乃一尙未解決之難題. 關於此方面 Siegel 之結果爲

$$\lim_{d \to \infty} \frac{\log (h(d) \log \varepsilon)}{\log d} = \frac{1}{2}.$$

但苦於對 $\log \varepsilon$ 之階所知不够,故無法得知 $h(d)$ 是否趨向無窮.

此二結果將於 §15 中證明之.

§ 14. 若干引理.

在下一節中將證明 Heilbronn-Siegel 定理. 在此證明中需要用到一些複變函數論的知識, 及第九章中所證明的關於 ζ 函數的某些簡單性質. 爲了方便起見,故將下一節中所需的知識分述如下:

1) 複變函數論中所徵引之定理爲:

定 理 1 (Cauchy 不等式). 若

$$f(s) = \sum_{n=0}^{\infty} a_n (s-a)^n$$

在 $|s-a| \leqslant r$ 中爲正則,且 $|f(s)| \leqslant M$, 則

$$|a_n| \leqslant M r^{-n} \qquad (n=0, 1, 2, \cdots).$$

(證明見普里瓦洛夫所著複變函數引論,第五章, §2, 第 8 段.)

2) 關於 ζ 函數所需的定理爲:

定 理 2. $\zeta(s)$ $(s = \sigma + it)$ 在半平面 $\sigma > 0$ 上爲一除 $s = 1$ 以外無處不正則的函數, 而 $s = 1$ 爲它的一次極點,在其上的留數爲 1. 又有

$$\left|\zeta(s)-\frac{1}{s-1}\right| \leqslant \frac{|s|}{\sigma} \qquad (\sigma>0) \tag{1}$$

成立（見定理 9.2.1）.

3）今引進另一函數

$$L_d(s)=\sum_{n=1}^{\infty}\left(\frac{d}{n}\right)\frac{1}{n^s} \qquad (\sigma>0),$$

此處 d 是一判別式. 顯然

$$L_d(1)=K(d).$$

定理 3. $L_d(s)$ 在右半平面 $\sigma>0$ 上表一正則函數，且適合

$$|L_d(s)|<\frac{|d|\cdot|s|}{\sigma} \qquad (\sigma>0), \tag{2}$$

及

$$0<L_d(1)<2+\log|d|. \tag{3}$$

證: 命 n_1, n_2 為任意二正整數，且 $n_2>n_1$. 則因

$$\left|\sum_{n_1\leqslant n\leqslant m}\left(\frac{d}{n}\right)\right|<|d|$$

對任何 $m>n_1$ 皆成立，故由定理 6.8.1 得

$$\left|\sum_{n_1\leqslant n\leqslant n_2}\left(\frac{d}{n}\right)\frac{1}{n^s}\right| \leqslant |d|\left(\sum_{n_1\leqslant n\leqslant n_2-1}\left|\frac{1}{n^s}-\frac{1}{(n+1)^s}\right|+\left|\frac{1}{n_2^s}\right|\right).$$

又

$$\left|\frac{1}{n^s}-\frac{1}{(n+1)^s}\right|=\left|s\int_n^{n+1}x^{-s-1}\,dx\right| \leqslant |s|\int_n^{n+1}x^{-\sigma-1}\,dx,$$

所以有

$$\left|\sum_{n_1\leqslant n\leqslant n_2}\left(\frac{d}{n}\right)\frac{1}{n^s}\right| \leqslant |d|\cdot|s|\left(\int_{n_1}^{n_2}x^{-\sigma-1}\,dx+|s|^{-1}n_2^{-\sigma}\right)\leqslant$$

$$\leqslant \frac{|d|\cdot|s|}{\sigma}n_1^{-\sigma} \qquad (\sigma>0). \tag{4}$$

由 (4) 可知，對於任何 $\sigma_0>0$, $L_d(s)$ 在半平面 $\sigma\geqslant\sigma_0$ 上的任何有限區域內為一致收斂，自然也為正則. 又因 σ_0 可取為任意小的正數，故 $L_d(s)$ 在半平面 $\sigma>0$ 內為一正則函數.

又在 (4) 中取 $n_1 = 1$, 而命 $n_2 \to \infty$, 可得 (2) 式.

由定理 10.1 及 $h(d) \geqslant 1$, $\log \varepsilon > 0$, 可知

$$L_d(1) = K(d) > 0.$$

又分

$$L_d(1) = \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) \frac{1}{n} = \sum_{n=1}^{|d|} \left(\frac{d}{n}\right) \frac{1}{n} + \sum_{n=|d|+1}^{\infty} \left(\frac{d}{n}\right) \frac{1}{n}$$

爲二部分,其第一部分

$$\left| \sum_{n=1}^{|d|} \left(\frac{d}{n}\right) \frac{1}{n} \right| \leqslant \sum_{n=1}^{|d|} \frac{1}{n} < 1 + \log |d|,$$

而第二部分,由 (4) 可知,

$$\left| \sum_{n=|d|+1}^{\infty} \left(\frac{d}{n}\right) \frac{1}{n} \right| \leqslant \frac{|d|}{|d|+1} < 1,$$

故得定理.

§ 15. Siegel 定理.

定理 1. 命 d 及 d_1 爲二判別式,及

$$f(s) = \zeta(s)\, L_d(s)\, L_{d_1}(s)\, L_{dd_1}(s),$$

則當 $\sigma > 1$ 時,有

$$f(s) = \sum_{n=1}^{\infty} a_n n^{-s}, \qquad a_1 = 1,\ a_n \geqslant 0 \qquad (n=2, 3, \cdots).$$

證: 當 $\sigma > 1$ 時, $\sum_{n=1}^{\infty} \frac{1}{n^s}$ 及 $\sum_{n=1}^{\infty} \left(\frac{d}{n}\right) \frac{1}{n^s}$ 皆爲絕對收斂, 且 $\frac{1}{n^s}$ 及 $\left(\frac{d}{n}\right) \frac{1}{n^s}$ 皆爲完全積性函數. 故由定理 5.4.4, 得

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \qquad L_d(s) = \prod_p \left(1 - \left(\frac{d}{p}\right) \frac{1}{p^s}\right)^{-1} \qquad (\sigma > 1).$$

若命

$$g(s, p) = \left\{ (1-p^{-s}) \left(1 - \left(\frac{d}{p}\right) p^{-s}\right) \left(1 - \left(\frac{d_1}{p}\right) p^{-s}\right) \left(1 - \left(\frac{dd_1}{p}\right) p^{-s}\right) \right\}^{-1},$$

則有

$$f(s) = \prod_p g(s, p) \qquad (\sigma > 1). \tag{1}$$

今 $\left(\frac{d}{p}\right)$, $\left(\frac{d_1}{p}\right)$, $\left(\frac{dd_1}{p}\right)$ 之值祇可能爲 0,1 或 -1. 當 $\left(\frac{d}{p}\right) = \left(\frac{d_1}{p}\right) = 1$

時，

$$g(s,p)=(1-p^{-s})^{-4}=\frac{1}{6}\sum_{m=0}^{\infty}(m+1)(m+2)(m+3)p^{-ms};$$

當 $\left(\frac{d}{p}\right)=-1, \left(\frac{d_1}{p}\right)=\pm 1$，或 $\left(\frac{d_1}{p}\right)=-1, \left(\frac{d}{p}\right)=\pm 1$ 時，

$$g(s,p)=(1-p^{-2s})^{-2}=\sum_{m=0}^{\infty}(m+1)p^{-2ms};$$

當 $\left(\frac{d}{p}\right), \left(\frac{d_1}{p}\right)$ 中有一爲 0，而另一個爲 $0, 1, -1$ 時，

$$g(s,p)=(1-p^{-s})^{-1}=\sum_{m=0}^{\infty}p^{-ms};$$

$$g(s,p)=(1-p^{-s})^{-2}=\sum_{m=0}^{\infty}(m+1)p^{-ms};$$

$$g(s,p)=(1-p^{-2s})^{-1}=\sum_{m=0}^{\infty}p^{-2ms}.$$

故對所有情形及任何素數 p，有 $a_1=1$，$a_{p^m}\geqslant 0$ $(m=1,2,\cdots)$，使

$$g(s,p)=\sum_{m=0}^{\infty}a_{p^m}p^{-ms} \qquad (\sigma>1) \tag{2}$$

成立。

由 (1) 及 (2) 得

$$f(s)=\prod_p\left(\sum_{m=0}^{\infty}a_{p^m}p^{-ms}\right) \qquad (\sigma>1). \tag{3}$$

今設 n 之標準分解式爲 $n=p_1^{q_1}\cdots p_l^{q_l}$. 定義

$$a_n=a_{p_1^{q_1}}\cdots a_{p_l^{q_l}},$$

故 a_n 對所有的自然數 n 皆有定義，且爲一積性函數，而 $a_1=1$，$a_n\geqslant 0$，再由定理 5.4.4 及 (3) 式可得

$$f(s)=\sum_{n=1}^{\infty}a_n n^{-s} \qquad (\sigma>1),$$

而 a_n 適合定理中的要求，也即 $a_1=1$，$a_n\geqslant 0$.

定理 2. 命 d 及 d_1 爲二基本判別式，$|d|>|d_1|>1$，如此則 dd_1 是一判別式. $f(s)$ 如定理 1 所定義，又命

$$\rho = L_d(1)\, L_{d_1}(1)\, L_{dd_1}(1)\,,$$

則當 $0 < \delta < a < 1$（δ 爲任一固定的小於 1 的正數）時，有

$$f(a) > \frac{1}{2} - \frac{C_1 \rho}{1-a}\, |dd_1|^{C_2(1-a)}\,,$$

此處 C_1, C_2 皆表祇與 δ 有關之正常數.

證：當 $|s-2| < 1$ 時，$f(s) - \frac{\rho}{s-1}$ 是正則的，故可把它展成 Taylor 級數如

$$f(s) - \frac{\rho}{s-1} = \sum_{m=0}^{\infty} (b_m - \rho)\,(2-s)^m\,, \tag{4}$$

此處

$$b_0 = f(2)\,,\qquad b_m = (-1)^m \frac{f^{(m)}(2)}{m!} \qquad (m=1,2,\cdots)\,.$$

而由定理 1，可知 $f(2) \geqslant 1$. $(-1)^m f^{(m)}(2) = \sum_{n=1}^{\infty} a_n\, n^{-2} \log^m n \geqslant 0$ $(m = 1, 2, \cdots)$ 亦卽

$$b_0 \geqslant 1\,,\qquad b_m \geqslant 0 \qquad (m=1,2,\cdots)\,. \tag{5}$$

由定理 14.2 及 14.3 可知 $f(s) - \frac{\rho}{s-1}$ 在右半平面 $\sigma > 0$ 上爲正則，故 (4) 式當 $|s-2| < 2$ 時也成立. 今將利用定理 14.1 以求出 $|b_m - \rho|$ 的上界. 爲此，先求 $\left|f(s) - \frac{\rho}{s-1}\right|$ 在圓周 $|s-2| = \frac{2-\delta}{\xi}$ 上的上界，此處 ξ 爲適合 $0<\xi<1$，且使 $1 < \frac{2-\delta}{\xi} < 2$ 的一數. 由定理 14.2 及定理 14.3 得

$$|f(s)| \leqslant \left(\frac{1}{|s-1|} + \frac{|s|}{\sigma}\right)\left(\frac{|s|}{\sigma}\right)^3 |dd_1|^2 \qquad (s \neq 1,\ \sigma > 0)\,. \tag{6}$$

今 $|s-2| = \frac{2-\delta}{\xi}$，故 $\frac{|s|}{\sigma} \leqslant \left(2 + \frac{2-\delta}{\xi}\right)\Big/\left(2 - \frac{2-\delta}{\xi}\right)$，$\frac{1}{|s-1|} \leqslant \left(\frac{2-\delta}{\xi} - 1\right)^{-1}$，故得

$$|f(s)| \leqslant C_3\, |dd_1|^2 \qquad \left(|s-2| = \frac{2-\delta}{\xi}\right),$$

其中 C_3 爲一僅與 δ 和 ξ 有關的正常數. 又由定理 14.3，可得

$$|\rho| \leqslant |dd_1|^2\,,$$

因此

$$\left|f(s) - \frac{\rho}{s-1}\right| \leqslant C_4\, |dd_1|^2\,,\qquad |s-2| = \frac{2-\delta}{\xi}\,, \tag{7}$$

而由最大模定理，可知 (7) 式於 $|s-2|\leqslant\frac{2-\delta}{\xi}$ 中也成立． 於是由定理 14.1 得

$$|b_m-\rho|\leqslant C_4\,|dd_1|^2\left(\frac{\xi}{2-\delta}\right)^m,\qquad m=0,1,2,\cdots. \tag{8}$$

今由 (4) 式以求 $f(a)$ 之下界．

$$f(a)=\frac{\rho}{a-1}+\sum_{m=0}^{m_0-1}(b_m-\rho)(2-a)^m+\sum_{m=m_0}^{\infty}(b_m-\rho)(2-a)^m,$$

由 (5) 可知

$$\sum_{m=0}^{m_0-1}(b_m-\rho)(2-a)^m\geqslant 1-\sum_{m=0}^{m_0-1}\rho(2-a)^m=1-\rho\frac{(2-a)^{m_0}-1}{1-a},$$

而由 (8)

$$\sum_{m=m_0}^{\infty}(b_m-\rho)(2-a)^m\geqslant -C_4\,|dd_1|^2\sum_{m=m_0}^{\infty}\left(\frac{\xi}{2-\delta}\right)^m(2-\delta)^m=$$

$$=-C_4\,|dd_1|^2\,\xi^{m_0}(1-\xi)^{-1}=-C_5\,|dd_1|^2\,\xi^{m_0},$$

故得

$$f(a)\geqslant 1-\rho\frac{(2-a)^{m_0}}{1-a}-C_5\,|dd_1|^2\,\xi^{m_0}. \tag{9}$$

今取 $m_0=\left[\frac{\log(2\,C_5\,|dd_1|^2)}{-\log\xi}\right]+1$，即得 $m_0<\frac{2\log|dd_1|}{-\log\xi}+C_6$ $(C_6>1)$ 及

$$C_5\,|dd_1|^2\,\xi^{m_0}<\frac{1}{2},$$

$$(2-a)^{m_0}<2^{C_7}\,|dd_1|^{\frac{2}{-\log\xi}\log(2-a)}\leqslant 2^{C_7}\,|dd_1|^{\frac{2}{-\log\xi}(1-a)}=$$

$$=C_1\,|dd_1|^{C_2(1-a)},$$

代入 (9) 式卽得定理．

定理 3 (Siegel)． 若 d 是一基本判别式，則對任一 $\varepsilon>0$，常有

$$\frac{1}{L_d(1)}=O(|d|^{\varepsilon}).$$

證： 不妨假定 $0<\varepsilon<\frac{1}{2}$，命

$$\left.\begin{aligned}&f(s)=\zeta(s)\,L_d(s)\,L_{d_1}(s)\,L_{dd_1}(s),\\&\rho=L_d(1)\,L_{d_1}(1)\,L_{dd_1}(1).\end{aligned}\right\} \tag{10}$$

d_1 的取法如下:

若有一基本判別式 d_1 使 $L_{d_1}(\sigma)$ 在 $1-\varepsilon<\sigma<1$ 中有一零點，卽取此 d_1 爲 (10) 中的 d_1，並以 a 表 $L_{d_1}(\sigma)$ 在此區間中的任一零點，則 $f(a)=0$.

若無基本判別式 d_1 使 $L_{d_1}(\sigma)$ 在 $1-\varepsilon<\sigma<1$ 中有零點，則任取一基本判別式 d_1. 此時，若 $f(\sigma)$ 在 $1-\varepsilon<\sigma<1$ 中有零點，則取 a 爲其中任一零點，仍有 $f(a)=0$; 若 $f(\sigma)$ 在此區間中也無零點，則取 a 爲 $1-\varepsilon<\sigma<1$ 中的任意一點，因 $f(\sigma)$ 在此區間中無零點，故有固定的符號；又由定理 14.3, 可知 $\rho>0$, 再因 $f(s)-\frac{\rho}{s-1}$ 在右半平面正則，所以當 σ 自左方趨近於 1 時，必須有 $f(\sigma)\to-\infty$, 因此可知 $f(\sigma)$ 在 $1-\varepsilon<\sigma<1$ 中取負值. 於是不論 d_1 與 a 如何取法，常有

$$f(a)\leqslant 0. \tag{11}$$

命 $|d|>|d_1|$, 由定理 2 $\left(取\ \delta=\frac{1}{2},\ 易見\ 0<\delta<1-\varepsilon<a<1\right)$, 得

$$\frac{C_1}{1-a}L_d(1)\,L_{d_1}(1)\,L_{dd_1}(1)\,|dd_1|^{C_2(1-a)}>\frac{1}{2},$$

此處 C_1, C_2 爲正絕對常數. 於是

$$\frac{1}{L_d(1)}<\frac{2C_1}{1-a}L_{d_1}(1)\,L_{dd_1}(1)\,|dd_1|^{C_2(1-a)}=$$
$$=C\,L_{dd_1}(1)\,|d|^{C_2(1-a)},$$

$C=\frac{2C_1}{1-a}L_{d_1}(1)\,|d_1|^{C_2(1-a)}$ 爲一與 d 無關之常數. 當 $|d|>|d_1|>1$ 時，有 $L_{dd_1}(1)\leqslant 2+\log|dd_1|<2\ (1+\log|d|)$, 又因 $1-a<\varepsilon$, 故得

$$\frac{1}{L_d(1)}<2C\,(1+\log|d|)\,|d|^{C_2\varepsilon}=O\,(|d|^{(C_2+1)\varepsilon}),$$

因 ε 是任意的，故得定理.

定理 4. 若 d 爲一判別式，則

$$\lim_{d\to-\infty}\frac{\log h(d)}{\log|d|}=\frac{1}{2},$$

$$\lim_{d\to\infty}\frac{\log\,(h(d)\log\varepsilon)}{\log d}=\frac{1}{2}.$$

證: 1) 若 d 爲基本判別式，因定理 3 及定理 14.3 得

$$C_8\,|d|^{-\varepsilon}<K(d)\leqslant 2+\log|d|<C_9\,|d|^{\varepsilon}, \tag{12}$$

再由定理 10.1 可知

$$C_{10}\,|d|^{\frac{1}{2}-\varepsilon}\leqslant h(d)\left\{\begin{matrix}1\\ \log\varepsilon\end{matrix}\right\}\leqslant C_{11}\,|d|^{\frac{1}{2}+\varepsilon},$$

此即定理。

2) 若 d 非基本判別式，而 $d=fm^2$, f 爲基本判別式。於是

$$K(d)=\prod_{p|m}\left(1-\left(\frac{f}{p}\right)\frac{1}{p}\right)K(f),$$

由於

$$\prod_{p|m}\left(1-\left(\frac{f}{p}\right)\frac{1}{p}\right)\leqslant 1$$

及

$$\prod_{p|m}\left(1-\left(\frac{f}{p}\right)\frac{1}{p}\right)\geqslant\prod_{p|m}\left(1-\frac{1}{p}\right)=\frac{\varphi(m)}{m}\geqslant C_{12}\,m^{-\varepsilon},$$

故得

$$C_{12}\,m^{-\varepsilon}K(f)\leqslant K(d)\leqslant K(f).$$

由 (12) 卽得

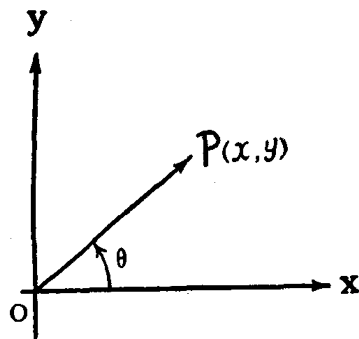
$$C_{13}\,|d|^{\frac{1}{2}-\varepsilon}\leqslant|d|^{\frac{1}{2}}K(d)\leqslant C_{14}\,|d|^{\frac{1}{2}}\,|f|^{\varepsilon}\leqslant C_{14}\,|d|^{\frac{1}{2}+\varepsilon}.$$

再由定理 10.1 而得定理。

第十三章

模變換

§1. 複虛數平面.



對應於一個複虛數

$$z = x + yi,$$

在平面上有一點 P，其坐標爲 (x, y)，此點爲 z 之寫像．顯然，此種表法是一對一的．從原點 O 到 P 作一射線 $\overrightarrow{OP}$ 稱爲矢量．故對應於一複虛數，有一從原點出發的矢量．

由 O 到 P 之距離 $\rho = \sqrt{x^2+y^2}$ 卽爲 z 之絕對値，也稱爲矢量 $\overrightarrow{OP}$ 之長度．$\overrightarrow{OP}$ 與 x 軸之夾角 θ 稱爲 z 之輻角．顯然可知

$$x = \rho\cos\theta, \qquad y = \rho\sin\theta.$$

ρ 及 θ 卽爲 (x, y)——平面上之極坐標．顯然可見

$$z = x + yi = \rho(\cos\theta + i\sin\theta) = \rho e^{i\theta}.$$

吾人常用下列符號：

$$|z| = \sqrt{x^2+y^2}, \qquad \arg z = \theta.$$

以 c 爲中心，$r(\geqslant 0)$ 爲半徑之圓，可以方程式

$$|z - c| = r$$

表之．而

$$|z| = 1$$

代表以 O 爲中心之單位圓．

今再硏究線性變換

$$z' = \frac{az+b}{cz+d}, \tag{1}$$

此處 a, b, c, d 爲常數（一般是複虛數），且

$$ad - bc \neq 0.$$

此變換將複虛數平面上之一點 $z\ (\neq -d/c)$ 變爲另一點 z'. 對應於 $z = -d/c$, 吾人引進一想像中之點,稱爲無窮遠點,以 $z' = \infty$ 表之。

今往討論之對象乃指複虛數平面加上無窮遠點者. 此對象稱爲函數論平面,在本章中或簡稱平面. $z = \infty$ 對應於 $z' = a/c$. 解 (1) 式得

$$z = \frac{-dz' + b}{cz' - a} \tag{2}$$

此仍爲一線性變換, 稱爲 (1) 之逆變換. 故變換 (1) 乃將函數論平面變爲其自己的一一對應.

在平面上放置一球,切於原點. 將此切點視爲"南極". 由"南極"作一垂直於平面之直線交球於另一點,視爲"北極". 自"北極"向平面上之一點 z 聯線, 交球面於一點, 如此建立起球面上諸點和平面上諸點的一一對應. 而無窮遠點則對應於"北極". 如此則所想像中的點, 一變而爲具體的點. 此球有時稱爲 Neumann 球.

§2. 線性變換之性質.

對應於一線性變換 A:

$$z' = \frac{az + b}{cz + d}, \tag{1}$$

有一方陣

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{2}$$

而此方陣之行列式之值 $ad - bc\ (\neq 0)$ 稱爲此變換之行列式. 但對應於不同的方陣可能有相同的線性變換,因爲

$$\begin{pmatrix} a\rho & b\rho \\ c\rho & d\rho \end{pmatrix}, \quad \rho \neq 0$$

所代表之變換和 (1) 完全相同. 不難證明, 除此情況之外, 無其他的方陣對應於變換 (1). 可取 ρ 使 $\rho^2(ad - bc) = 1$, 故常可假定有行列式爲 1 之方陣代表線性變換 A. 極易證明對應於一線性變換僅有二行列式爲 1 之方陣對應之, 卽

$$\begin{pmatrix} \pm a & \pm b \\ \pm c & \pm d \end{pmatrix}.$$

若另有一線性變換 B:

$$z''=\frac{a'z'+b'}{c'z'+d'},\tag{3}$$

則得一線性變換 C

$$z''=\frac{a'(az+b)+b'(cz+d)}{c'(az+b)+d'(cz+d)}$$

$$=\frac{(a'a+b'c)z+a'b+b'd}{(c'a+d'c)z+c'b+d'd}.\tag{4}$$

此變換之方陣

$$\begin{pmatrix} a'a+b'c & a'b+b'd \\ c'a+d'c & c'b+d'd \end{pmatrix}$$

定義爲二方陣 $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 之積,記之爲

$$\begin{pmatrix} a'a+b'c & a'b+b'd \\ c'a+d'c & c'b+d'd \end{pmatrix}=\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

變換 (4) 也稱爲變換 (3) 及 (1) 之積,記之如 $C=BA$.

但需注意者,BA 並不一定等於 AB. 吾人以 A^{-1} 表 A 之逆變換.

變換

$$z'=z$$

稱爲單位變換,以 E 代表之. 可得 $A\cdot A^{-1}=A^{-1}\cdot A=E$.

定義* **1.** 若一組線性變換其中包有單位變換, 且其中二變換之積仍在其中,其中任一變換之逆變換也在其中,則此組變換稱爲做成一羣.

例 1. 所有的線性變換成一羣.

例 2. 所有的實係數的線性變換成一羣.

例 3. 所有的實係數而行列式爲正的線性變換成一羣.

例 4. 取 a, b, c, d 爲整數,且 $ad-bc=\pm 1$, 則所得出的線性變換也成一羣.

例 5. 取 a, b, c, d 爲複虛整數 (即 $a=a'+a''i$, a', a'' 都是整數), 所得出的線性變換也成一羣.

定義 2. 若 z_0 由 A 變爲其自己,則此點稱爲 A 之定點.

---

*成羣之三性質有其互相關聯性,但本書僅以簡而易用爲滿足.

一般說來，一個變換有二不同的定點，（即 $z' = z$）．即二次方程

$$cz^2 + (d - a)z - b = 0 \tag{5}$$

之二根．

若 z_1，z_2 爲此式之二根，則該變換可以寫成標準形式

$$\frac{z'-z_1}{z'-z_2} = \lambda \frac{z-z_1}{z-z_2}. \tag{6}$$

欲定此 λ，可取 $z = \infty$，則 $z' = a/c$，故

$$\lambda = \frac{a-cz_1}{a-cz_2}.$$

易證此 λ 適合於二次方程

$$\lambda + \frac{1}{\lambda} = \frac{a^2+d^2+2bc}{ad-bc} = \frac{(a+d)^2}{ad-bc} - 2. \tag{7}$$

若 $|\lambda| = 1$，$\lambda \neq 1$，此變換稱爲橢圓的．

若 λ 是實數而 $\neq \pm 1$，則稱爲雙曲的．

若 λ 爲複數，$|\lambda| \neq 1$，則稱爲等緯角的（Loxodromic）．

若 $c = 0$，而 $d - a \neq 0$，則有一定點變爲無窮．如取 $z_2 = \infty$，則 (6) 式之形式變爲

$$z' - z_1 = \lambda(z - z_1). \tag{8}$$

若二定點相吻合，即 $z_1 = z_2$，則

$$(a - d)^2 + 4bc = 0,$$

即

$$(a + d)^2 + 4(bc - ad) = 0. \tag{9}$$

適合此條件之變換稱爲拋物的．代入 (7) 式，得 $\lambda = 1$．標準式 (6) 今變爲

$$\frac{1}{z'-z_1} = \frac{1}{z-z_1} + k, \tag{10}$$

此處 $z_1 = (a - d)/2c$，$k = 2c/(a + d)$．

特別當 $c = 0$，$a - d = 0$，則此定點變爲無窮，而變換變爲

$$z' = z + k, \qquad k = b/a.$$

若有一變換續用若干次而成爲單位變換，則稱爲有限次變換，最小之次數使

其成爲單位變換者,稱爲該變換之週期. 續用 (10) 及 (6) n 次,各得

$$\frac{1}{z'-z_1}=\frac{1}{z-z_1}+nk$$

$$\frac{z'-z_1}{z'-z_2}=\lambda^n\frac{z-z_1}{z-z_2}.$$

故拋物,雙曲及等緯角變換,都不能有週期. 僅當橢圓變換,且 $\lambda^n=1$ 時爲然. 其週期卽爲最小之正整數 n 使 $\lambda^n=1$ 者.

當 $n=2$ 時,則 $\lambda=-1$, 週期爲 2 之變換稱爲對合.

§3. 線性變換下之幾何性質.

定義.

$$(z_1\,z_2\,z_3\,z_4)=\frac{z_3-z_1}{z_2-z_3}\bigg/\frac{z_4-z_1}{z_2-z_4}$$

稱爲四點 z_1, z_2, z_3, z_4 之交比.

定理 1. 線性變換使交比不變.

證: 命

$$z_i'=\frac{az_i+b}{cz_i+d},$$

則

$$z_i'-z_j'=\frac{(ad-bc)(z_i-z_j)}{(cz_i+d)(cz_j+d)},$$

故

$$(z_1'\,z_2'\,z_3'\,z_4')=(z_1\,z_2\,z_3\,z_4).$$

有一線性變換存在,變任與三點 z_1, z_2, z_3 爲任意三點 z_1', z_2', z_3'. 此變換之形式可具體地寫出來

$$\frac{z'-z_1'}{z'-z_2'}=\frac{z_3'-z_1'}{z_3'-z_2'}\,\frac{z_3-z_2}{z_3-z_1}\,\frac{z-z_1}{z-z_2},\tag{1}$$

或

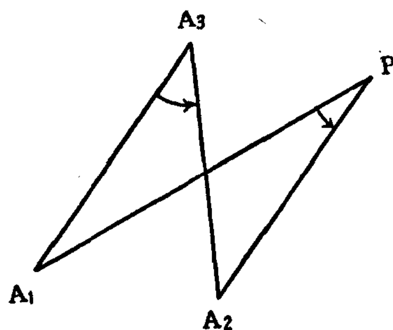
$$\frac{z_3'-z_2'}{z_3'-z_1'}\,\frac{z'-z_1'}{z'-z_2'}=\frac{z_3-z_2}{z_3-z_1}\,\frac{z-z_1}{z-z_2},$$

亦卽

$$(z_1'\,z_2'\,z_3'\,z')=(z_1\,z_2\,z_3\,z).\tag{2}$$

若有一線性變換具有上述性質，由定理 1，當 z 給定後，則 z' 必適合 (2) 式. 即 z' 唯一確定. 故具此性質的變換是唯一的. 換言之，(2) 乃線性變換之一般形式.

若 A_1, A_2, A_3, P 各表 z_1, z_2, z_3, z 諸點，則



$$\arg(z_1\,z_2\,z_3\,z) = \angle A_1\,PA_2 - \angle A_1\,A_3\,A_2,$$

角之方向一如圖中箭頭所示.

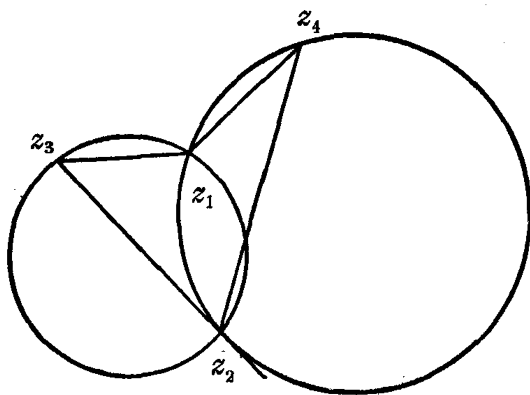
由此可見，若交比是實數，則

$$\angle A_1\,PA_2 - \angle A_1\,A_3\,A_2$$

等於 π 之倍數. 故 P 在經過 A_1, A_2, A_3 三點之圓上.

若 $(z_1\,z_2\,z_3\,z)$ 是實數，則 (2) 式中 $(z_1'\,z_2'\,z_3'\,z')$ 也爲實數，即當 z 在過三點 z_1, z_2, z_3 之圓上時，z' 亦在過 z_1', z_2', z_3' 之圓上，且反之亦眞. 故已證明線性變換變圓爲圓. 但須注意者：通常將直線看成直徑爲無窮大之圓.

定理 2. 線性變換使二圓之交角不變. 即若二圓之交角爲 θ 度，則經線性變換另得二圓其交角仍爲 θ 度.



證：命 z_1, z_2 爲二圓之交點. 在 z_1 點附近，二圓上各取一點 z_3, z_4. 則交比之輻角

$$\arg\,(z_3\,z_4\,z_1\,z_2),$$

即爲 $\angle z_3\,z_2\,z_4 - \angle z_3\,z_1\,z_4$. 當 z_3 及 z_4 都趨近於 z_1 時，即得二圓之交角. 由於交比之不變性，故得定理.

§4. 實變換.

今往討論 a, b, c, d 爲實數之線性變換

$$z' = \frac{az+b}{cz+d}, \qquad ad - bc \neq 0.$$

但今不能取實數 ρ 使

$$\rho^2(ad-bc)=1;$$

而僅能取得 ρ 使

$$\rho^2(ad-bc)=\pm 1.$$

今後不妨假定

$$ad-bc=\pm 1.$$

顯然行列式為 $+1$ 之諸實線性變換成一羣,此羣以 $\mathfrak{R}$ 表之. 顯然,此羣中之變換變實數軸為其自己. 對任意三實數,有一實變換將其變為任與之三實數.

定理 1. $\mathfrak{R}$ 將上半平面(即 $y>0$)變為其自己.

證: 命 $z'=x'+iy'$, $z=x+iy$, $\bar{z}=x-iy$, 則

$$2iy'=\frac{az+b}{cz+d}-\frac{a\bar{z}+b}{c\bar{z}+d}$$

$$=\frac{2(ad-bc)iy}{|cz+d|^2}, \tag{1}$$

故得所需.

定義 1. 上半平面內中心在 x 軸上之半圓謂之測地線.

由定理 1 及定理 3.2, 可得:

定理 2. $\mathfrak{R}$ 中之變換將測地線變為測地線.

在上半平面中任取二點 z_1, z_2. 若有一 $\mathfrak{R}$ 中之變換變 z_1 及 z_2 各為 z_1', z_2', 則顯然有

$$(z_1\ \bar{z}_1\ z_2\ \bar{z}_2)=(z_1'\ \bar{z}_1'\ z_2'\ \bar{z}_2')$$

即

$$\left|\frac{z_2-z_1}{\bar{z}_1-z_2}\right|^2=\left|\frac{z_2'-z_1'}{\bar{z}_1'-z_2'}\right|^2.$$

取 $z_2=z+\Delta z$, $z_1=z$, 並命 $\Delta z\to 0$, 則得出

$$\left|\frac{dz}{2y}\right|^2=\left|\frac{dz'}{2y'}\right|^2,$$

即

$$\frac{dx^2+dy^2}{y^2}=\frac{dx'^2+dy'^2}{y'^2}.$$

由此可見，$\mathfrak{R}$ 中的變換使長度元素

$$\frac{\sqrt{dx^2+dy^2}}{y} \tag{2}$$

不變．與此長度元素相當之面積元素爲

$$\frac{dx\,dy}{y^2}, \tag{3}$$

經 $\mathfrak{R}$ 中的變換亦不變．如讀者缺乏微分幾何之常識，可用直接法以證出 (2) 及 (3) 經 $\mathfrak{R}$ 中之變換不變．

定理 3. 命 z_1, z_2 爲上半平面之兩點，c 爲連接此二點之一曲線* (全在上半平面中)，則使

$$\int_C \frac{\sqrt{dx^2+dy^2}}{y}$$

取極小値者，乃 c 爲測地線之情況．

證： 作一中心在 x 軸上之圓，且經過 z_1, z_2 二點．命其中心爲 $(t, 0)$，則圓之方程可以寫成

$$x = t + \rho\cos\theta,$$
$$y = \quad \rho\sin\theta.$$

設 $\theta=\theta_1$ 及 θ_2 時，$z=z_1$ 及 z_2．該曲線 C 之方程可以寫成

$$\left.\begin{aligned} x &= t+\rho(\theta)\cos\theta,\\ y &= \quad \rho(\theta)\sin\theta,\end{aligned}\right\}\quad \rho(\theta_1)=\rho(\theta_2)=\rho,\ 0<\theta_1<\theta_2<\pi,$$

則

$$\int_C \frac{\sqrt{dx^2+dy^2}}{y} =$$

$$=\int_{\theta_1}^{\theta_2}\frac{\sqrt{(\rho'(\theta)\cos\theta-\rho(\theta)\sin\theta)^2+(\rho'(\theta)\sin\theta+\rho(\theta)\cos\theta)^2}}{\rho(\theta)\sin\theta}\,d\theta=$$

$$=\int_{\theta_1}^{\theta_2}\sqrt{1+\left(\frac{\rho'(\theta)}{\rho(\theta)}\right)^2}\,\frac{d\theta}{\sin\theta}\geqslant$$

$$\geqslant\int_{\theta_1}^{\theta_2}\frac{d\theta}{\sin\theta}=\log\frac{\tan\frac{1}{2}\theta_2}{\tan\frac{1}{2}\theta_1}.$$

*假定此曲線是連續的，並有連續切線．

此式證明了：僅當 $\rho'(\theta)=0$ 時取等號，卽當 $\rho(\theta)=\rho$ 是一常數時該積分之值極小。

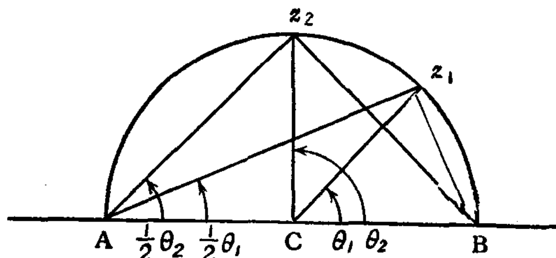


圖 1

此定理之證明不但證明了定理，且證明了沿測地線該積分之值爲

$$\log \frac{\tan \frac{1}{2}\theta_2}{\tan \frac{1}{2}\theta_1}.$$

其意義爲：假定過 z_1, z_2 之測地線交 x 軸於 A, B，其中心爲 C，則

$$\tan \frac{1}{2}\theta_1 = \frac{Bz_1}{z_1A}, \qquad \tan \frac{1}{2}\theta_2 = \frac{Bz_2}{z_2A}.$$

故

$$\log\left(\frac{\tan \frac{1}{2}\theta_2}{\tan \frac{1}{2}\theta_1}\right) = \log|(B\,A\,z_2\,z_1)|.$$

定義 2. 定理 3 中之極小值稱爲此兩點之非歐長度.

定義 3. 三測地線所範圍之弧三角形，本章中卽統稱爲三角形.

定理 4. 三角形 ABC 之非歐面積

$$\iint \frac{dx\,dy}{y^2}$$

等於 $\pi - \angle A - \angle B - \angle C$.

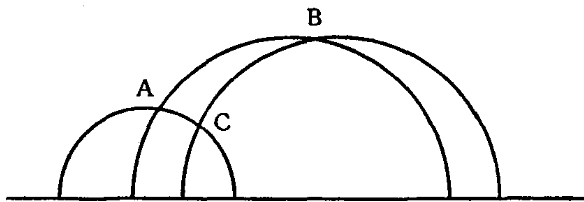


圖 2

證：1) 先研究 $\angle B = \angle C = 0$ 之情况（如圖 3 所示）. 不難證明，有一實線性變換，將 B 點變爲無窮，C 點變爲 1，D 點變爲 -1（或此變換將 C 點變爲 -1，D 點變爲 1），且所對應的行列式爲正*. 則圖 3 變爲圖 4. 設 A 點之

*將 B, C, D 變爲 $\infty, \pm 1, \mp 1$ 的實變換爲

$$z' = \pm \frac{(D-2B+C)z + (BC-2DC+DB)}{(C-D)z + (D-C)B},$$

而其對應的行列式之值爲

$$\pm 2(D-C)(C-B)(B-D).$$

坐標爲 (x_0, y_0)，則

$$\int_{x_0}^{1}\int_{\sqrt{1-x^2}}^{\infty}\frac{dx\,dy}{y^2}=$$

$$=\int_{x_0}^{1}\frac{dx}{\sqrt{1-x^2}}=\sin^{-1}x\Big|_{x_0}^{1}=$$

$$=\frac{\pi}{2}-\sin^{-1}x_0=\pi-\angle A.$$

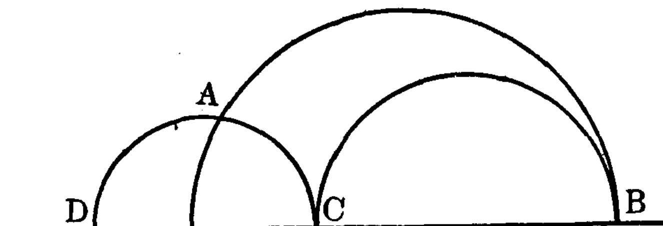


圖 3

2). 若 $\angle C=0$，用一次實變換將 C 點變爲無窮，得圖 5. 由 1) 得

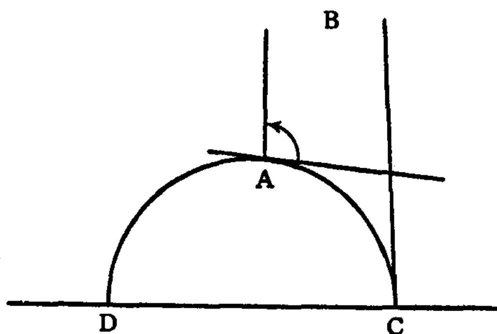


圖 4

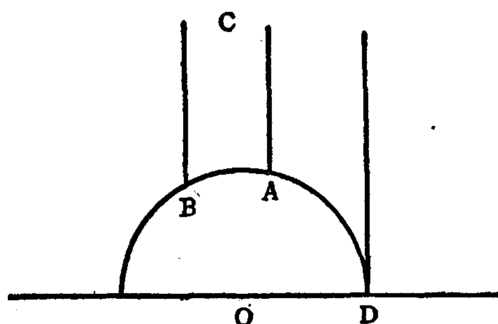


圖 5

$$\triangle ABC=\triangle BDC-\triangle ADC=(\pi-\angle B)-[\pi-(\pi-\angle A)]=\pi-\angle A-\angle B.$$

3). 若 $\angle A, \angle B, \angle C$ 皆不爲 0，如圖 6. 則由 2) 得

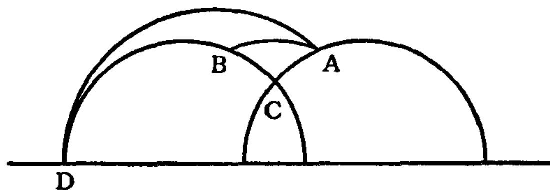


圖 6

$$\triangle ABC=\triangle ADC-\triangle ABD=$$
$$=(\pi-\angle C-\angle A-\angle BAD)-[\pi-(\pi-\angle B)-\angle BAD]=$$
$$=\pi-\angle A-\angle B-\angle C.$$

由此定理可知三角形三內角之和不大於二直角，其值可取 0 與 π 之間之任一值.

以上所述，乃著名的 Н. Л. Лобачевский 幾何之模型，乃模函數發展到自型函數之一重要工具.

§5. 模變換.

定義. 若 a, b, c, d 是整數,且 $ad-bc=1$, 則變換

$$z'=\frac{az+b}{cz+d} \tag{1}$$

稱爲模變換.

易見模變換成一羣.

由 §2 (7) 可知

$$\lambda+\lambda^{-1}=(a+d)^2-2.$$

此二次方程之判別式爲

$$[(a+d)^2-2]^2-4=(a+d)^2[(a+d)^2-4].$$

在討論中,不妨假定 $a+d\geqslant 0$. 若不然可將 a, b, c, d 換爲 $-a, -b, -c, -d$.

1) 若 $a+d>2$, 則得雙曲變換,有二個實數定點: 此二定點乃二次方程

$$cz^2+(d-a)z-b=0$$

之根. 此二次方程有有理根之條件爲

$$(d-a)^2+4bc=(a+d)^2-4=u^2,$$

u 乃一整數. 但因 $x^2-y^2=4$ 之解爲 $x=\pm 2$, $y=0$ 而無其他,故雙曲模變換之定點,一定是有理係數二次方程之根,而非有理數. 此種數稱爲二次代數數.

2) 若 $a+d=2$, 則 $\lambda=1$, 而得拋物變形

$$\frac{1}{z'-(a-1)/c}=\frac{1}{z-(a-1)/c}+c.$$

若 $c=0$, 則 $a=d=1$, 而得

$$z'=z+b.$$

前者以有理數 $(a-1)/c$ 爲定點,後者以 ∞ 爲定點.

3) 若 $a+d=1$, 則

$$\lambda^2+\lambda+1=0,$$

該變換之 λ 爲 $\rho=e^{2\pi i/3}=\dfrac{-1+\sqrt{-3}}{2}$ 或 ρ^2, 而固定點爲

$$z_1=\frac{a+\rho^2}{c},\qquad z_2=\frac{a+\rho}{c}.$$

而標準形式爲

$$\frac{z'-(a+\rho^2)/c}{z'-(a+\rho)/c}=\rho\,\frac{z-(a+\rho^2)/c}{z-(a+\rho)/c}.$$

此爲一橢圓變換,週期爲 3. 將 ρ 換爲 ρ^3 得另一週期爲 3 之橢圓變換.

4) $a+d=0$, 則 λ 之方程式爲 $(\lambda+1)^2=0$, 卽 $\lambda=-1$, 而定點爲

$$cz^2-2az-b=0$$

之根,卽

$$z=\frac{a\pm i}{c}.$$

而標準形式爲

$$\frac{z'-(a+i)/c}{z'-(a-i)/c}=-\frac{z-(a+i)/c}{z-(a-i)/c}.$$

此爲一橢圓變換, 週期爲 2.

總之有:

定理 1. 若 $a+d=0$, 則模變換 (1) 代表一對合;若 $a+d=\pm1$, 則代表一週期爲 3 之變換; 若 $a+d=\pm2$, 則得抛物變換,其定點是有理數或無窮; 若 $|a+d|>2$, 則得雙曲變換, 其定點在實軸上,並且是二次代數數.

§ 6. 基域.

定義 1. 上半平面之二點 z, z' 如能有一模變換將 z 變爲 z', 則此二點謂之相似,以 $z\sim z'$ 表示之.

顯然有

(i) $z\sim z$;

(ii) 若 $z\sim z'$, 則 $z'\sim z$;

(iii) 若 $z\sim z'$, $z'\sim z''$, 則 $z\sim z''$.

在上半平面作一域

$$D:\begin{cases}-\frac{1}{2}\leqslant x<\frac{1}{2},\\ x^2+y^2>1 \quad 當\quad x>0 \text{ 時},\\ x^2+y^2\geqslant 1 \quad 當\quad x\leqslant 0 \text{ 時}.\end{cases}$$

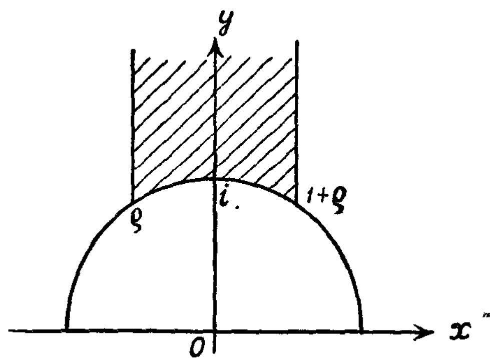


圖 7

定義 2. 在 D 上之點稱爲既約點. D 稱爲基域. 故 D 乃一三角形,其三角之度數爲 $\left(0, \frac{\pi}{3}, \frac{\pi}{3}\right)$.

定理 1. 無二既約點可以彼此相似.

證: 若 z, z' 爲二不同的既約點, 且

$$z' = \frac{az+b}{cz+d}.$$

則由 §4 (1) 可知

$$y' = \frac{y}{|cz+d|^2},$$

今有

$$\begin{aligned}|cz+d|^2 &= c^2 z\bar{z} + cd(z+\bar{z}) + d^2 = \\ &= c^2(x^2+y^2) + 2cdx + d^2 \geqslant \\ &\geqslant c^2 - |cd| + d^2 > 1.\end{aligned}$$

但須除去可能的例外: $c = \pm 1, d = 0$ 或 $c = 0, d = \pm 1$ 或 $c = d = 1$. 故將可能的例外情況除去後常有

$$y' < y.$$

當 $c = d = 1$ 時, 僅當 $z = \rho$ 時有 $|cz+d|^2 = 1$. 由於 $a - b = 1$ 及 $\rho^2 + \rho + 1 = 0$, 則

$$z' = \frac{a\rho+b}{\rho+1} = -\frac{a\rho+b}{\rho^2} = -a\rho^2 - b\rho = -\rho^2 + b.$$

故 $I(z') = \frac{\sqrt{3}}{2}$. 若 $z' \in D$, 則 $z' = \rho$, 而與 $z' \neq \rho$ 矛盾.

但

$$z = \frac{dz'-b}{-cz'+a},$$

故常有

$$y < y',$$

同樣須除去可能的例外: $c = \pm 1, a = 0$ 或 $c = 0, a = \pm 1$.

不可能同時有 $y > y'$ 及 $y < y'$. 故僅須研究以下的情形:

(i) $c = 0, \quad a = d = 1;$

(ii) $c = 1, \quad a = d = 0.$

在第一種情況下，

$$z' = z + b, \qquad b \neq 0.$$

卽 $x' = x + b$. $|x' - x| \geqslant 1$, 故 z, z' 不能都在 D 中.

在第二種情況下，$b = -1$, 卽

$$z' = -\frac{1}{z}.$$

$$|z'| \cdot |z| = 1.$$

卽若 $|z| > 1$, 則 $|z'| < 1$, 卽 z' 不能爲旣約點. 若 $|z'| > 1$, 則 z 不能爲旣約點. 若 $|z| = 1$, 則 z 僅能在由 ρ 到 i 之圓弧上,而 $z'(= -1/z)$ 在由 $\rho + 1$ 到 i 之圓弧上. 若 $z \neq i$, 則 z' 並非旣約點;若 $z = i$, 則 $z' = i = z$, 此與假設矛盾.

定理 2. 在長方形 $-\frac{1}{2} \leqslant x < \frac{1}{2}$, $y \geqslant \gamma$ $(\gamma > 0)$ 中,相似於一定點之點數有限. 亦卽將長方形中諸點分爲相似點組,則每組中點數有限.

證: 假定 $z = x + yi$,

$$z' = \frac{az+b}{cz+d},$$

則已知

$$y' = \frac{y}{|cz+d|^2} = \frac{y}{c^2(x^2+y^2)+2cdx+d^2}.$$

若 $y' \geqslant \gamma$, 則

$$c^2(x^2 + y^2) + 2cdx + d^2 \leqslant \frac{y}{\gamma},$$

卽

$$(cx + d)^2 + c^2 y^2 \leqslant \frac{y}{\gamma}.$$

顯然祇能有有限對整數 c, d 適合此式.

假定 (c', d') 是如此的一對,且 $(c', d') = 1$, 則適合於

$$ad' - bc' = 1$$

之所有解答 (a, b) 可以表成

$$a = a' + mc', \qquad b = b' + md',$$

此處 a', b' 是一固定解,卽 $a'd' - b'c' = 1$, 而 m 爲任一整數,故

$$z' = \frac{az+b}{c'z+d'} = \frac{a'z+b'}{c'z+d'} + m.$$

僅有唯一的 m，使$-\frac{1}{2}\leqslant x'<\frac{1}{2}$. 故對一對 (c', d') $((c', d')=1)$，僅有一組 a, b 使$-\frac{1}{2}\leqslant x'<\frac{1}{2}$，故在長方形中相似於 z 之點數有限.

定理 3. 上半平面之任一點相似於唯一的既約點.

證: 命 $z=x_0+y_0 i$, $y_0>0$.

取唯一的整數 m 使

$$-\frac{1}{2}\leqslant x_0+m<\frac{1}{2}.$$

命

$$z'=z+m.$$

若 $|z'|>1$, 則 z' 是既約點,無須證明. 若 $|z'|=1$, 而在 ρ 至 i 之弧上,即為既約點,若在 $1+\rho$ 至 i 之弧上,可用 $-\frac{1}{z}$ 而變為上之情況. 若$|z'|<1$,則使

$$z''=-\frac{1}{z'},$$

而

$$y''=\frac{y_0}{|z'|^2}>y_0.$$

取 m' 使

$$z'''=z''+m', \qquad -\frac{1}{2}\leqslant x'''<\frac{1}{2}.$$

若 z''' 還不是既約點,用同樣方法,做出 $z^{IV}=-\frac{1}{z'''}$.

由是得 $z', z''', \cdots$ 等都在長方形

$$-\frac{1}{2}\leqslant x<\frac{1}{2}, \qquad y>y_0$$

內,由定理 2 已知其個數僅能為有限.

故任一點一定與一既約點相似. 又由定理 1 已知不能有二既約點相似. 此證明了本定理.

為了更能欣賞此定理之重要性,可用直接方法以證明以下二條可由本定理直接得出之結果.

習題 1. 凡

$$z=\frac{a+i}{c},\qquad a^2+bc+1=0$$

皆相似於 i.

習題 2. 凡

$$z=\frac{a+\rho}{c},\qquad a(1-a)-bc=1$$

皆相似於 ρ.

§7. 基域網.

定理 1. 若 z 非一模變換之定點之一，而 U, V 爲二不同之模變換，則

$$Uz\neq Vz,$$

Uz 代表變換 U 將 z 變成之點.

證：若 $Uz=Vz$, 則

$$z=U^{-1}Vz.$$

而得 z 是定點.

定理 2. 作基域之所有的映像，所得出之諸三角形塡滿上半平面，且無重復部分.

證：本定理上半部分可由定理 6.3 知之. 若 U 及 V 爲二不同之模變換，將基域 D 變爲有公共部分之二三角形，則 $U^{-1}V$ 必變 D 爲一與 D 有公共部分之三角形. 命 z 爲公共部分中之一點，則 D 中必有一點與之相似，以其都在 D 中故不可能.

此定理可以堆磚爲喩. 在普通空間中，可以等大之正方形之磚塡滿空間. 而所謂等大磚之意義卽爲此磚可以"搬"佔另一磚之地位.

現在之"基域"乃磚之模形，"搬動"乃模變換，而上定理卽謂如此之磚可以塡滿上半平面. 此乃非歐幾何學之說法. 如重用此種說法，基域之意義可更明顯，且易於推廣.

基域之定義作如下之更動：上半平面之一域具次之性質者謂之基域：

(i) 任一點必與其中之一點相似；

(ii) 其中任二點不相似.

在上半平面中任取一點 z，非一模變形之定點. 在平面上作此點之相似點

$$z_1, z_2, \cdots.$$

作 (z, z_i) 之垂直平分線，卽其上之點與 z 及 z_i 之非歐距離相等者． 捨棄在 z_i 一面之部分． 所剩下之部分，卽成一基域．（其證明，讀者試補出之，並試求出取 $z=2i$ 時所得出之基域．）

此僅能提供説明：Лобачевский 幾何不但有理論上之重要性，在數論中及函數論中也有其實踐的意義．

所可注意者：週期爲 2 之橢圓變換之定點在角度爲 $\frac{\pi}{3}$ 之二角所夾之邊上．週期爲 3 之橢圓變換之定點有六個三角形以之爲公頂．有無數個邊經過拋物定點．雙曲定點不能爲三角形之頂點（不能在邊上更爲明顯）．

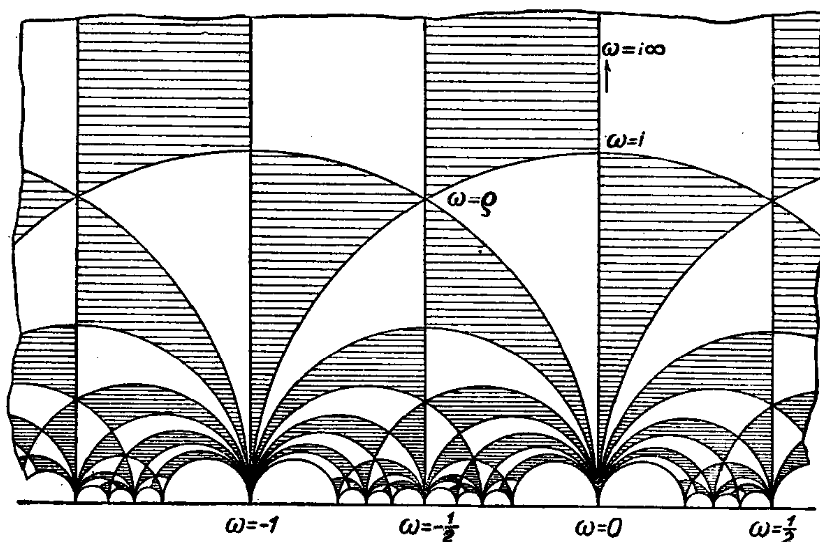


圖 8

§8. 模羣之構造．

今以 S 代表 $z'=z+1$，T 代表 $z'=-\frac{1}{z}$． 則 S^{-1} 代表 $z'=z-1$．此三變換將基域變爲其相鄰之三域，反之將基域之鄰域變爲基域之變換必爲 S, T 或 S^{-1} 之一．

命 M 爲任一模變換，z 爲基域 D 內部之任一點． 以曲線連接 z 與 Mz，使此曲線不過頂點． 假定所過之域依次名爲

$$D, D_1, D_2, \cdots, D_n(=MD).$$

又命將 D 變爲 D_i 之模變換爲 M_i，則 $M_1=S, T$ 或 S^{-1}． 假定 M_k 可由 S 及 T 之乘方之積表出． 因爲 M_k^{-1} 將 D_k 變爲 D，D_{k+1} 是 D_k 的鄰域，故

M_k^{-1} 將 D_{k+1} 變爲 D 的鄰域 D'_{k+1}, 但 D'_{k+1} 經過 $M'^{-1}(=S, T$ 或 $S^{-1})$ 變爲 D. 卽

$$M'^{-1}\ M_k^{-1} D_{k+1} = M'^{-1}\ D'_{k+1} = D,$$

亦卽

$$M_k\ M'\ D = D_{k+1}.$$

故 $M_{k+1} = M_k M'$ 可由 S 及 T 之乘方之積表出,而 M 亦然. 由此已證明:

定理 1. 任一模變換可由 S 及 T 之乘方之積表出.

定理 1 之具體意義爲: 若

$$M = S^{m_1}\ TS^{m_2}\ TS^{m_3} \cdots TS^{m_\nu},$$

則

$$z' = m_1 - \frac{1}{m_2} - \frac{1}{m_3} - \frac{1}{m_4} - \cdots - \frac{1}{m_\nu + z}.$$

此顯出模變換與連分數之關係.

易知 $T^2 = E$, $(ST)^3 = E$.

注意: 若擴大模變換之定義:

$$z' = (az+b)/(cz+d), \qquad ad - bc = \pm 1,$$

則可得類似之結果

$$z' = m_1 + \frac{1}{m_2} + \frac{1}{m_3} + \cdots + \frac{1}{m_\nu + z}.$$

§ 9. 二次定正型.

命 ω 表一在上半平面中之複數, ρ 爲實數 > 0. 作二次型

$$F(x, y) = \rho(x - \omega y)(x - \bar{\omega} y) = \rho x^2 - \rho(\omega + \bar{\omega}) xy + \rho\omega\bar{\omega}\ y^2.$$

若用一次模變換

$$\omega = (a\omega' + b)/(c\omega' + d),$$

則上式變成

$$\rho((c\omega'+d)x - (a\omega'+b)y)((c\bar{\omega}'+d)x - (a\bar{\omega}'+b)y)/|c\omega'+d|^2 =$$
$$= \rho(dx - by - \omega'(-cx+ay))(dx - by - \bar{\omega}'(-cx+ay))/|c\omega'+d|^2,$$

卽得

$$\rho(X - \omega' Y)(X - \bar{\omega}' Y)/|c\omega' + d|^2,$$

此處

$$X = dx - by, \qquad Y = -cx + ay.$$

故得

$$\left\{\rho, -\rho(\omega+\bar{\omega}), \rho\omega\bar{\omega}\right\} \sim \left\{\frac{\rho}{|c\omega'+d|^2}, -\frac{\rho(\omega'+\bar{\omega}')}{|c\omega'+d|^2}, \frac{\rho\omega'\bar{\omega}'}{|c\omega'+d|^2}\right\}. \quad (1)$$

其中須注意者:

$$\omega - \bar{\omega} = \frac{\omega' - \bar{\omega}'}{|c\omega' + d|^2}.$$

由任一二次定正型

$$\{\alpha, \beta, \gamma\}$$

出發,此處假定 α, β, γ 是實數 $(\alpha>0)$ 及 $\beta^2 - 4\alpha\gamma < 0$. 與 (1) 式左邊相比較,卽得

$$\rho = \alpha, \qquad \omega = \frac{-\beta + \sqrt{\beta^2 - 4\alpha\gamma}}{2\alpha}.$$

由 (1) 並假定 ω' 在基域之中,則得

$$-1 \leqslant \omega' + \bar{\omega}' < 1, \begin{cases} \omega'\bar{\omega}' > 1, & 若\ \omega' + \bar{\omega}' > 0, \\ \omega'\bar{\omega}' \geqslant 1, & 若\ \omega' + \bar{\omega}' \leqslant 0. \end{cases}$$

以 $\{\alpha', \beta', \gamma'\}$ 代 (1) 之右邊,則得

$$-1 < \frac{\beta'}{\alpha'} \leqslant 1, \begin{cases} \frac{\gamma'}{\alpha'} > 1', & 若\ \beta' < 0, \\ \frac{\gamma'}{\alpha'} \geqslant 1, & 若\ \beta' \geqslant 0. \end{cases}$$

即得

$$-\alpha' < \beta' \leqslant \alpha' < \gamma'$$

或

$$0 \leqslant \beta' \leqslant \alpha' \leqslant \gamma'.$$

此已將定理 12.2.3 推廣至實二次定正型.

習題 1. 定出經一非單位模變換而不變的二次型之標準形式 (答: x^2+y^2, $x^2 + xy + y^2$).

§10. 二次不定型.

今論實係數之二次不定型

$$F = \{a, b, c\} = ax^2 + bxy + cy^2 = a(x - \omega_1 y)(x - \omega_2 y), \quad d = b^2 - 4ac > 0.$$

假定 $a>0$，且 ω_1，ω_2 皆非有理數，以 ω_1、ω_2 二點之連線爲直徑作圓．此圓稱爲此型之基圓，其方程爲

$$a(x^2+y^2)+bx+c=0.$$

此圓必與無限多個三角形相交．蓋由定理 6.2 之證明，可以看出，對每一有理點 $-\frac{d'}{c'}$ 皆有無限多個模變換將其變爲無限遠點．亦即有無限多個三角形以此有理點爲其一頂點．但每一實數之附近有無限多個有理點．故得所云．若與基圓相交之無限多個三角形中有一爲基域，則此二次型稱爲既約二次型．顯然任一二次不定型必與一既約二次型相似，此可由定理 6.3 直接推出．

一既約二次型之基圓必包有 ρ 或 $1+\rho$，即 $\left(\frac{1}{2},\frac{\sqrt{3}}{2}\right)$，$\left(-\frac{1}{2},\frac{\sqrt{3}}{2}\right)$ 二點中至少必有一點在圓內．亦即

$$a\left(a\pm\frac{b}{2}+c\right)<0, \tag{1}$$

以 $c=(b^2-d)/4a$ 代入，則得

$$4a^2\pm 2ab+b^2<d$$

或

$$3a^2+(a\pm b)^2<d. \tag{2}$$

沿基域 D_0 之弧向左右出發，將基圓所經過之三角形列之爲

$$\cdots, D_{-2}, D_{-1}, D_0, D_1, D_2, \cdots.$$

命 M_i 是一模變換變 D_0 爲 D_i，則由 F 經 M_i 所得之二次型 F_i 與 F 相似．如是得一二次不定型鏈

$$\cdots, F_{-2}, F_{-1}, F, F_1, F_2, \cdots. \tag{3}$$

因 M_i^{-1} 爲一實變換，故 F 之二實根經 M_i^{-1} 後變爲 F_i 之二實根．故 M_i^{-1} 將 F 之基圓變爲 F_i 之基圓．但 F 之基圓通過 D_i，故 F_i 之基圓通過 D_0，此即說明 (3) 爲一列既約二次型鏈．

D_1 可能是 D_0 之一鄰域，但如基圓經過頂點 $1+\rho$，則 D_1 可能是圖 9 中所

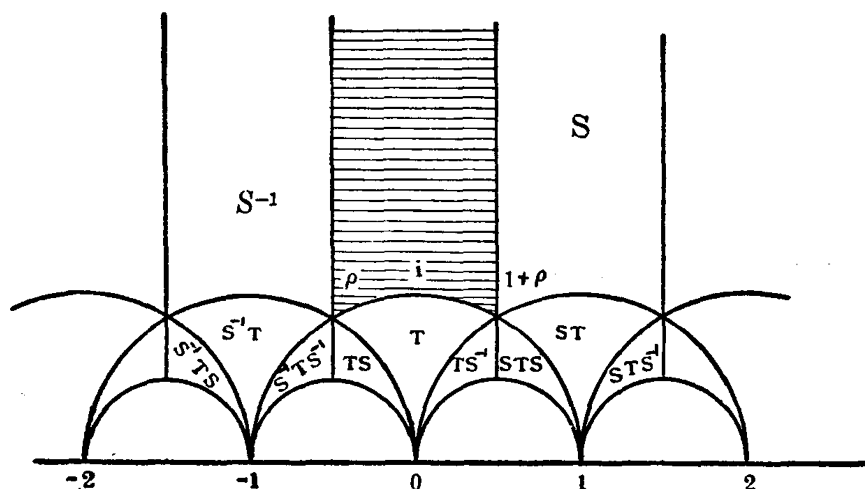


圖 9

描述的 STS 域，同理，也可能是 $S^{-1}TS^{-1}$ 域．如是，該鏈中相鄰之二型必可由變換

$$S,\ S^{-1},\ T,\ STS,\ S^{-1}TS^{-1}$$

之一得之．卽若命$\{a,b,c\}$爲鏈中之一型，則此型之前後二型必爲下述五型之一：

$$\{a,\pm 2a+b,\ a\pm b+c\},\quad \{c,-b,a\},\quad \{a\pm b+c,\ b\pm 2c,\ c\}.$$

今進一步，討論整係數之二次型：由 (2) 可知既約二次型之個數僅能有有限個．因此在鏈中僅有有限個不同的型．

定理 1. 以 ω_1,ω_2 二根爲定點之雙曲變換爲

$$\begin{pmatrix} \frac{1}{2}(t-bu) & -cu \\ au & \frac{1}{2}(t+bu) \end{pmatrix}, \tag{4}$$

此處

$$t^2-du^2=4.$$

且無其他模變換有此性質．

證：此雙曲變換之定點爲

$$au\,x^2+\left(\frac{t+bu}{2}-\frac{t-bu}{2}\right)x+cu=0,$$

卽

$$ax^2+bx+c=0$$

之根，其後一部份易證.

定理 2. 雙曲變換 (4) 使 $\{a, b, c\}$ 不變，且無其他.

證: 易證二次型

$$a\left(\frac{1}{2}(t-bu)x-cuy\right)^2+b\left(\frac{1}{2}(t-bu)x-cuy\right)\left(aux+\frac{1}{2}(t+bu)y\right)+$$
$$+c\left(aux+\frac{1}{2}(t+bu)y\right)^2$$

中 x^2, xy, y^2 之係數各爲 a, b, c.

定理 3. 在鏈 (3) 中發生周而復始的現象.

證: 已知 (3) 中僅有有限個不相同者. 命 m 爲最小正整數使 $F_m = F$ 者. 命 M 爲模變換變 F 爲 F_m 者. 則 M^{-1} 使基圓不變，故 M^{-1} 變 D_{m+1} 爲 D_1, 故得 $F_{m+1} = F_1, \cdots$.

例. $d = 37\times 4$.

由 $(1, 0, -37)$ 開始之鏈爲

$(1, 0, -37), (1, 2, -36), (1, 4, -33), (1, 6, -28), (1, 8, -21),$
$(1, 10, -12), (1, 12, -1), (-1, -12, 1), (-1, -10, 12), \cdots$
$(-1, 12, 1), (1, -12, -1), (1, -10, -12), \cdots, (1, -2, -36).$

由 $(3, 2, -12)$ 開始之鏈爲

$(3, 2, -12), (3, 8, -7), (4, -6, -7), (4, 2, -9),$
$(4, 10, -3), (-3, -10, 4), (-3, -4, 11), (-3, 2, 12),$
$(-3, 8, 7), (-4, -6, 7), (-4, 2, 9), (-4, 10, 3),$
$(3, -10, -4), (3, -4, -11).$

§11. 二次不定型的極小值.

現回到實係數之二次型: 相似用廣義的定義，即 $ad - bc = -1$ 之變換也列入. 比前所述之結果還可以更具體些.

定理 1. 一二次不定型必相似於一型，其基圓直徑之一端 $-1 < \omega_1' < 0$, 而另一端 $\omega_2' > 1$.

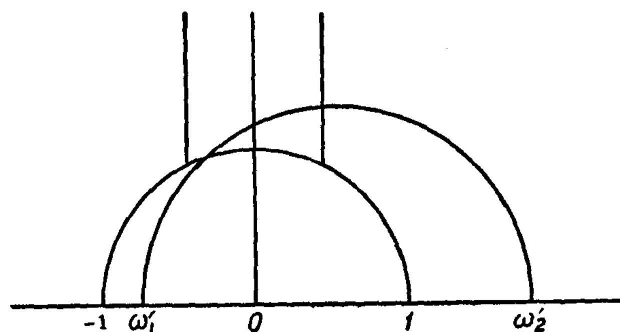
證: 由上節，任一二次不定型必與一既約二次型相似. 作此既約二次型之基圓. 若其與由 ρ 到 i 之弧相交，則有三種情況:

1) $-1<\omega_1'<0$, $\omega_2'>1$;

2) $\omega_1'<-1$, $0<\omega_2'<1$;

3) $-1<\omega_2'<0$ 則 $\omega_1'<-2$.

①



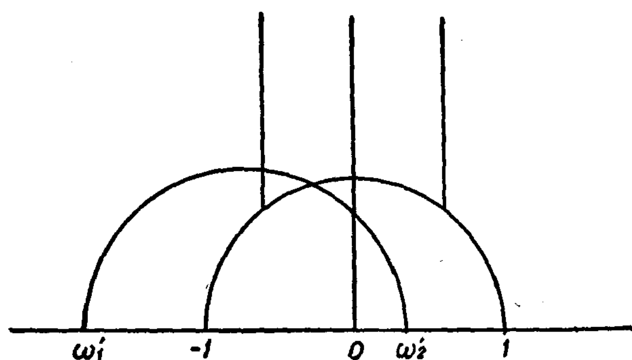
對 1) 不須加證.

對 2) 用變換 $z'=z+1$ 卽得所求.

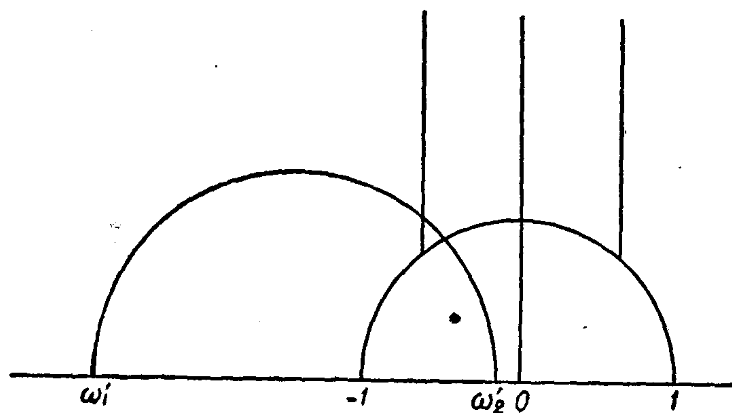
對 3) 命

$$z''=-z'-1,$$

②



③



則

$$-1 < \omega_2'' < 0, \quad 而 \quad \omega_1'' = -\omega_1' - 1 > 1,$$

卽得所求.

若其與由 i 到 $1+\rho$ 之弧相交，則由變換 $z' = -z$ 而歸結爲上述情形. 若不與由 ρ 到 $1+\rho$ 之弧相交,則必有一模變換 $z' = z + m$ 使其歸結爲上述二情形之一. 故定理已明.

今設

$$F_0 = \alpha_0 x_0^2 + \beta_0 x_0 y_0 + \gamma_0 y_0^2,$$

其二根爲 $\omega_1^{(0)}$, $\omega_2^{(0)}$, 且適合

$$\omega_1^{(0)} > 1, \qquad -1 < \omega_2^{(0)} < 0.$$

將 $\omega_1^{(0)}$ 及 $-\frac{1}{\omega_2^{(0)}}$ 依連分數展開之,

$$\omega_1^{(0)} = d_1 + \frac{1}{d_2} + \frac{1}{d_3} + \cdots, \qquad -\frac{1}{\omega_2^{(0)}} = d_0 + \frac{1}{d_{-1}} + \frac{1}{d_{-2}} + \cdots.$$

變換

$$x_0 = d_1 x_1 + y_1, \qquad y_0 = x_1$$

變 F_0 爲

$$F_1 = \alpha_1 x_1^2 + \beta_1 x_1 y_1 + \gamma_1 y_1^2,$$

其二根爲

$$\omega_1^{(1)} = d_2 + \frac{1}{d_3} + \cdots, \qquad -\frac{1}{\omega_2^{(1)}} = d_1 + \frac{1}{d_0} + \cdots.$$

一般言之,在 F_{i-1} 上用

$$x_{i-1} = d_i x_i + y_i, \qquad y_{i-1} = x_i,$$

則得

$$F_i = \alpha_i x_i^2 + \beta_i x_i y_i + \gamma_i y_i^2.$$

其二根爲

$$\omega_1^{(i)} = d_{i+1} + \frac{1}{d_{i+2}} + \cdots, \qquad -\frac{1}{\omega_2^{(i)}} = d_i + \frac{1}{d_{i-1}} + \frac{1}{d_{i-2}} + \cdots.$$

二根之差等於

$$\frac{\sqrt{d}}{\alpha_i}=\omega_1^{(i)}-\omega_2^{(i)}=\left(d_{i+1}+\frac{1}{d_{i+2}}+\cdots\right)+\left(\frac{1}{d_i}+\frac{1}{d_{i-1}}+\cdots\right).$$

命 $L(F)$ 爲對所有之整數 (x_0, y_0)

$$|\alpha_0 x_0^2+\beta_0 x_0 y_0+\gamma_0 y_0^2|$$

之極小值。顯然有

$$L(F)\leqslant|\alpha_i|=\frac{\sqrt{d}}{\left(d_{i+1}+\frac{1}{d_{i+2}}+\cdots\right)+\left(\frac{1}{d_i}+\frac{1}{d_{i-1}}+\cdots\right)}.$$

命

$$\min_i\left(\left(d_{i+1}+\frac{1}{d_{i+2}}+\cdots\right)+\left(\frac{1}{d_i}+\frac{1}{d_{i-1}}+\cdots\right)\right)=U,$$

則

$$L(F)\leqslant\frac{\sqrt{d}}{U}$$

有無窮個解.

若諸 d_i 皆爲 1, 則得

$$1+\frac{1}{1}+\frac{1}{1}+\cdots=\frac{1}{2}(1+\sqrt{5}),\quad \frac{1}{1}+\frac{1}{1}+\cdots=\frac{1}{2}(\sqrt{5}-1),$$

卽得

$$U=\sqrt{5}.$$

故

$$|ax^2+bxy+cy^2|\leqslant\frac{\sqrt{d}}{\sqrt{5}}$$

有無窮個解。

但若 $\omega_1=\frac{1}{2}(1+\sqrt{5})$, $\omega_2=-\frac{1}{2}(\sqrt{5}-1)$, 則得

$$F=(x^2-xy-y^2)\sqrt{\frac{d}{5}}.$$

對所有的整數 x, y

$$|F(x,y)|\geqslant\sqrt{\frac{d}{5}}.$$

又若有一 $d_i\geqslant 3$, 則

$$[d_i, d_{i+1},\cdots]+[0, d_{i-1},\cdots]\geqslant 3>\sqrt{5},$$

因此

$$L(F) \leqslant \frac{\sqrt{d}}{3}.$$

又若有一 $d_i = 2$，則（$1 \leqslant d_{i-1} \leqslant 2$）

$$[2, d_{i+1}, d_{i+2}, \cdots] \geqslant 2$$

及

$$[0, d_{i-1}, \cdots] \geqslant \frac{1}{d_{i-1}+\frac{1}{d_{i-2}}} \geqslant \frac{1}{2+\frac{1}{1}} = \frac{1}{3},$$

故

$$[d_i, d_{i+1}, \cdots] + [0, d_{i-1}, \cdots] \geqslant 2 + \frac{1}{3} > \sqrt{5}.$$

切實言之,我們有:

定理 2. 吾人常有

$$L(F) \leqslant \sqrt{\frac{d}{5}}.$$

若

$$L(F) = \sqrt{\frac{d}{5}},$$

則 F 相似於

$$\sqrt{\frac{d}{5}}\,(x^2 \pm xy - y^2).$$

第十四章

整數矩陣及其應用

§1. 引言. 今將先討論二行二列的方陣，以概括地介紹全章之內容. 其中有一部分已見之於第十三章,但爲了完整及易於了解起見,稍有重復。

今往討論二行二列之方陣

$$M=\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tag{1}$$

此處 a, b, c, d 是整數. 組成方陣之數稱爲方陣之元素. 元素皆爲零之方陣謂之零方陣,以 0 表之。

$$ad-bc$$

稱爲 M 之行列式. 若此值等於 ± 1, 則 M 謂之模方陣; 若此值等於 1, 則 M 謂之正模方陣. 行列式不等於零之方陣謂之非奇異方陣,不然謂之奇異方陣.

二方陣

$$A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad B=\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$$

之積的定義是

$$\begin{pmatrix} aa_1+bc_1 & ab_1+bd_1 \\ ca_1+dc_1 & cb_1+dd_1 \end{pmatrix}, \tag{2}$$

並以記號 AB 表之. 顯然 AB 之行列式等於 A 之行列式乘 B 之行列式. 又二模方陣之積仍爲一模方陣,二正模方陣之積仍爲一正模方陣.

設 k 是一整數,定義

$$k\cdot\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} ka & kb \\ kc & kd \end{pmatrix}.$$

方陣

$$I=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

稱爲單位方陣. 對任一方陣 M, 常有 $MI=IM=M$.

若 $AB=I$, 則 B 稱爲 A 之逆,以 A^{-1} 記之. 易知模方陣 $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 有逆方陣存在,且

$$A^{-1}=\pm\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$ (當 A 爲正模方陣時取正號,否則取負號.)

顯然 $AA^{-1}=A^{-1}A=I$. 又從 $AB=I$ 兩邊取行列式, 可知 A 若有逆方陣, 則 A 爲模方陣. 故方陣 A 有逆方陣之充要條件是 A 爲模方陣.

在正模方陣中有兩個極重要之方陣

$$S=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{3}$$

及

$$T=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{4}$$

極易算出: 對任一整數 $m\ \left(\gtreqless 0\right)$,常有

$$S^m=\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \tag{5}$$

及

$$T^2=-I. \tag{6}$$

定理 1. 任一正模方陣可由 S 及 T 之乘方乘積表出之;換言之,正模方陣所成之羣可由 S 及 T 演出之.

證: 假定

$$M=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{7}$$

是一正模方陣. 若 $a=0$, 則 $b\neq 0$. 由

$$\begin{pmatrix} 0 & b \\ c & d \end{pmatrix}T=\begin{pmatrix} -b & 0 \\ -d & c \end{pmatrix}$$

可知在討論中不妨假定 $a\neq 0$. 又因

$$MT^2=-M,$$

故也不妨假定 $a>0$. 又可設

$$0\leqslant b<a. \tag{8}$$

蓋可取整數 q, 使 $0\leqslant aq+b<a$, 而方陣

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} a & aq+b \\ c & cq+d \end{pmatrix} \tag{9}$$

卽適合 (8) 式.

今對 a 行歸納法. 若 $a=1$, 則由 (8) 得出 $b=0$, 因而 $d=1$. 而

$$\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}=TS^{-c}T^{-1}.$$

故 (7) 乃 S 及 T 之乘方乘積.

今設當 $0<a<k$ 時,所有適合於 (8) 之方陣 (7) 皆爲 S 及 T 之乘方乘積. 則對正模方陣

$$\begin{pmatrix} k & l \\ s & t \end{pmatrix}, \quad 0\leqslant l<k$$

(因爲 $k>1$, 故 l 顯然大于 0),由

$$\begin{pmatrix} k & l \\ s & t \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} l & -k \\ t & -s \end{pmatrix}$$

再用 (9) 之方法,可知此式之右邊爲 S 及 T 之乘方乘積. 故得定理.

附註: 正模方陣也可由二方陣

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ 及 } \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \tag{10}$$

之乘方乘積表出之. 蓋由於

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

故也.

定理 2. 任一模方陣可由二方陣

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ 及 } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{11}$$

之乘方乘積表出之,亦卽模方陣所成之羣可由此二方陣演出之.

證: 模方陣 M 如非正模方陣,則

$$M\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

卽爲正模方陣. 因之由定理 1 的附註,可知模方陣可由三方陣

$$\begin{pmatrix}1&1\\0&1\end{pmatrix},\ \begin{pmatrix}1&0\\1&1\end{pmatrix},\ \begin{pmatrix}0&1\\1&0\end{pmatrix}$$

之乘方乘積表出之. 但

$$\begin{pmatrix}1&0\\1&1\end{pmatrix}=\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix},$$

故得定理.

定義 1. 如有一模方陣 U 使二方陣 M, N 間有下之關係:

$$M = UN,$$

則謂方陣 N 左結合於方陣 M. 以 $M\overset{L}{=}N$ 表之.

左結合關係顯然有次之三性質: (i) $M\overset{L}{=}M$ (反身性); (ii) 若 $M\overset{L}{=}N$, 則 $N\overset{L}{=}M$ (對稱性); (iii) 若 $M\overset{L}{=}N$, $N\overset{L}{=}P$, 則 $M\overset{L}{=}P$ (傳遞性).

右結合之定義可仿此得出,故不再贅述.

定理 3. 任一方陣必左結合於方陣

$$\begin{pmatrix}a&0\\c&d\end{pmatrix},\quad a\geqslant 0,\quad d\geqslant 0. \tag{12}$$

若 $a>0$, 則 $0\leqslant c<a$.

證: 給與一方陣

$$M=\begin{pmatrix}a&b\\c&d\end{pmatrix},$$

必有整數 r, s 使

$$rb+sd=0,\qquad (r, s)=1.$$

又必有整數 u, v 使

$$rv-su=1.$$

於是

$$U=\begin{pmatrix}r&s\\u&v\end{pmatrix}$$

爲一正模方陣,而

$$UM=\begin{pmatrix}a_1&0\\c_1&d_1\end{pmatrix}.$$

如 $a_1\leqslant 0$, 則以 $\begin{pmatrix}-1&0\\0&1\end{pmatrix}$ 乘之, 可使 $a_1\geqslant 0$; 同法可使 $d_1\geqslant 0$. 因之任一方陣必左結合於如下形式之方陣

$$\begin{pmatrix}a&0\\c&d\end{pmatrix},\quad a\geqslant 0,\quad d\geqslant 0.$$

若 $a>0$，則可取 q 使 $0\leqslant qa+c<a$，卽得

$$\begin{pmatrix}1&0\\q&1\end{pmatrix}\begin{pmatrix}a&0\\c&d\end{pmatrix}=\begin{pmatrix}a&0\\qa+c&d\end{pmatrix}.$$

故得定理.

定義 2. 形如 (12) 之方陣謂之左結合標準形式.

定理 4. 任一非奇異方陣之左結合標準形式是唯一的.

證: 首先注意非奇異方陣之左結合標準形式 $\begin{pmatrix}a&0\\c&d\end{pmatrix}$ 中之 a, d 皆不爲零. 今若

$$\begin{pmatrix}s&t\\u&v\end{pmatrix}\begin{pmatrix}a&0\\c&d\end{pmatrix}=\begin{pmatrix}a_1&0\\c_1&d_1\end{pmatrix},\quad sv-tu=\pm 1.$$

則由 $td=0$ 得 $t=0$. 再由 $sa=a_1>0$, $vd=d_1>0$ 及 $sv=\pm 1$, 可得 $s=v=1$. 更由 $ua+c=c_1$, $0\leqslant c<a$, $0\leqslant c_1<a_1=a$, 可知 $u=0$. 故得定理.

習題. 讀者自己研究奇異方陣之情況.

定義 3. 如有二模方陣 U 及 V 使

$$UMV=N,$$

則謂方陣 M 與 N 相似，以 $M\sim N$ 記之. 此相似關係顯然也有反身，對稱，傳遞等三性質.

定理 5. 任一方陣必與一形如

$$\begin{pmatrix}a_1&0\\0&a_1a_2\end{pmatrix},\quad a_1\geqslant 0,\quad a_2\geqslant 0 \tag{13}$$

之方陣相似.

證: 給與一方陣

$$M=\begin{pmatrix}a&b\\c&d\end{pmatrix}.$$

若 M 之元素全爲零，則定理顯然，故不妨假定 $a\neq 0$, 亦不妨假定 $a>0$. 今先證: M 必與一形如

$$\begin{pmatrix}a_1&b_1\\c_1&d_1\end{pmatrix},\quad a_1\mid(b_1,\ c_1,\ d_1)$$

之方陣相似. 今用歸納法證明此點. 當 $a=1$ 時，此乃顯然. 當 $a>1$ 時，若 $a\nmid b$, 則可取整數 q 使 $0<aq+b<a$, 而

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} aq+b & * \\ * & * \end{pmatrix},$$

此處為首之元素為小於 a 之正整數. 又若 $a|b$ 而 $a \nmid c$, 則亦有整數 q' 使 $0 < aq' + c < a$, 而

$$\begin{pmatrix} q' & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} aq'+c & * \\ * & * \end{pmatrix},$$

此處為首之元素亦為小於 a 之正整數. 最後,若 $a|(b, c)$, 但 $a \nmid d$, 命 $c = c'a$, 則

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -c' & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} a & (1-c')b+d \\ * & * \end{pmatrix},$$

而 $a \nmid \{(1-c')b+d\}$, 此化為 $a \nmid b$ 之情形. 故由歸納法明所欲證.

今 $a_1|(b_1, c_1, d_1)$, 命 $b_1 = a_1 b_2$, $c_1 = a_1 c_2$, $d_1 = a_1 d_2$, 由是

$$\begin{pmatrix} 1 & 0 \\ -c_2 & 1 \end{pmatrix}\begin{pmatrix} a_1 & a_1 b_2 \\ a_1 c_2 & a_1 d_2 \end{pmatrix}\begin{pmatrix} 1 & -b_2 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} a_1 & 0 \\ 0 & a_1(d_2-b_2 c_2) \end{pmatrix}.$$

顯然可設 $a_1 > 0$, 因不然以 $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ 乘之卽得. 同樣可設 $a_2 = d_2 - b_2 c_2 \geqslant 0$. 故得定理.

定義 4. 形如 (13) 之方陣稱為相似標準形式.

總述以上之結果: 由定理 2 已知任一模方陣可由二方陣

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

之乘方乘積表出之. 由

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} c & d \\ a & b \end{pmatrix}$$

及

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} b & a \\ d & c \end{pmatrix},$$

可知 $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ 及其逆之作用是將一方陣之兩行或兩列互換. 又由

$$\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} a \pm c & b \pm d \\ c & d \end{pmatrix}$$

及

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} a & b \pm a \\ c & d \pm c \end{pmatrix},$$

可知 $\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$ 或其逆 $\begin{pmatrix}1 & -1\\0 & 1\end{pmatrix}$ 之作用是於第一行加上或減去第二行(即對應的元素分別相加減，以後同此)，或於第二列加上或減去第一列. 如此數種手續稱爲初等變換. 故定理 5 亦可改述爲: 經初等變換後，可將一方陣變爲相似標準形式.

由於方陣中諸元素之最大公約數經初等變換後不變，因之由定理 5,

$$(a, b, c, d) = a_1.$$

又

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc = \pm a_1^2 a_2.$$

因而可得

定理 6. 任一方陣之相似標準形式是唯一的.

§ 2. 矩陣之積.

命 $a_{11}, a_{12}, \cdots, a_{mn}$ 皆表整數,

$$A = \begin{pmatrix} a_{11} \cdots a_{1n} \\ a_{21} \cdots a_{2n} \\ \cdots\cdots\cdots\cdots \\ a_{m1} \cdots a_{mn} \end{pmatrix}$$

稱爲一 m 行 n 列的矩陣，或稱爲 $m \times n$ 矩陣，而以 $A^{(m,n)}$ 記之. 若 $m = n$, 則逕以 $A^{(n)}$ 記之，並稱爲 n 級的方陣. 又以 B 表一 $n \times l$ 矩陣.

$$B = \begin{pmatrix} b_{11} \cdots b_{1l} \\ b_{21} \cdots b_{2l} \\ \cdots\cdots\cdots\cdots \\ b_{n1} \cdots b_{nl} \end{pmatrix}$$

矩陣 A 乘 B 的乘積定義爲

$$AB = C = \begin{pmatrix} c_{11} \cdots c_{1l} \\ c_{21} \cdots c_{2l} \\ \cdots\cdots\cdots\cdots \\ c_{m1} \cdots c_{ml} \end{pmatrix}, \qquad c_{rs} = \sum_{t=1}^{n} a_{rt} b_{ts} \ (r = 1, \cdots, m; s = 1, \cdots, l). \quad (1)$$

由定義易見只有當 A 的列數與 B 的行數相等時，AB 纔有意義. 又易見當 AB 和 BA 都有意義時，AB 並不一定等於 BA. 若 $AB = BA$, 則稱 A, B 是可交換的. 但常有 $(AB)D = A(BD)$.

如 A, B 爲方陣，則 AB 之行列式等於 A 之行列式乘以 B 之行列式.

如一方陣之行列式不爲零,則此方陣稱爲非奇異方陣,不然謂之奇異方陣.

行列式爲 ± 1 之方陣稱爲模方陣,而行列式爲 1 者稱爲正模方陣. 易證二模方陣之積仍爲一模方陣,二正模方陣之積仍爲一正模方陣.

方陣

$$\Lambda = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

除對角線上之元素外,其餘之元素皆爲零,稱爲對角線方陣,並簡記之爲 $\Lambda = [\lambda_1, \lambda_2, \cdots, \lambda_n]$. 特如 $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 1$, 即

$$\Lambda = I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

稱爲單位方陣. 顯然對任一方陣 A 常有 $AI = IA = A$.

若方陣 A, B 間有下之關係

$$AB = I,$$

則稱 B 爲 A 之逆方陣,並以 $B = A^{-1}$ 記之.

於方陣 $A(=A^{(n)})$ 中除去第 i 行第 j 列諸元素,但不變動其他元素之位置,所得 $(n-1)$ 級方陣之行列式稱爲 a_{ij} 之餘子式;餘子式前冠以符號 $(-1)^{i+j}$ 後,稱爲代數餘子式,以 A_{ij} 記之. 命

$$A_0 = \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix},$$

A_0 即爲於 A 中以 a_{rs} 之代數餘子式 A_{rs} 代 a_{sr} 後所得之方陣,稱爲 A 之伴隨方陣. 易證

$$AA_0 = A_0A = aI,$$

此處 a 表 A 之行列式. 故若 A 爲模方陣,則 A 有逆方陣存在,且 $A^{-1} = \pm A_0$. 反之,若 A 有逆方陣,則 A 爲模方陣.

若 $AB = I$, 則由 $B = (\pm A_0 A)B = \pm A_0(AB) = \pm A_0$, 可知逆方陣是唯一的,且 $AA^{-1} = A^{-1}A = I$. 且若 A, B 皆有逆方陣,則 $(AB)^{-1} = B^{-1}A^{-1}$.

1 行 n 列的矩陣 $(x_1, \cdots, x_n)$（其中之元素 $x_1, \cdots, x_n$ 有時不限定爲整數）稱爲矢量，並以 $x=(x_1, \cdots, x_n)$ 記之。所當注意者：此處矢量之記號請勿與最大公約數之記號 $(x_1, \cdots, x_n)=d$ 相混淆。以後凡單獨寫 $(x_1, \cdots, x_n)$ 時卽表矢量，而 $(x_1, \cdots, x_n)=d$ 表示最大公約，並常以 x, y 等字母表示含有 n 個元素的矢量.

方程

$$y = xB \ (B = B^{(n,l)}) \tag{2}$$

卽代表線性方程組

$$y_i = \sum_{j=1}^{n} x_j b_{ji}, \quad 1 \leqslant i \leqslant l.$$

若 $n=l$ 而 B 非奇異的，則 (2) 稱爲變換. 對應於整數 $x_1, \cdots, x_n$ 有整數 $y_1, \cdots, y_n$，但反之則不一定. 但若 B 爲模方陣，則當 $y_1, \cdots, y_n$ 爲整數時，$x_1, \cdots, x_n$ 亦爲整數，此時稱變換 (2) 爲模變換.

例 1. 設 $r \neq 1$. 命 $y_1 = -x_r$, $y_r = x_1$, $y_i = x_i (i \neq 1, i \neq r)$. 此爲一模變換，其所對應之模方陣卽爲將 I 之第 1 行乘 -1 後與第 r 行互換後所得之方陣（或第 r 列乘 -1 後與第 1 列互換後所得之方陣），以 E_r 記之.

$$E_r = \begin{pmatrix} 0 & 0 & \cdots & 1 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ -1 & 0 & \cdots & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} r. \tag{3}$$
$$\qquad\qquad\qquad r$$

例 2. 設 $r \neq 1$. 命 $y_i = x_i \ (i \neq r)$, $y_r = x_r + x_1$. 此亦爲一模變換，其所對應之模方陣爲

$$V_r = \begin{pmatrix} 1 & 0 & \cdots & 1 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}, \tag{4}$$
$$\qquad\qquad\qquad r$$

卽爲將 I 之第 r 行加到第 1 行去後所得之方陣（或第 1 列加到第 r 列去後所得之方陣）.

易證 V_r 可表爲 V_2 及 E_i 之乘積. 實際上，若 $r > 2$，則

$$V_r = E_2 E_r E_2 V_2 E_2 E_r E_2. \tag{5}$$

今證明如下：命

$$t = \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix},$$

則有

$$E_2 t = \begin{pmatrix} t_2 \\ -t_1 \\ t_3 \\ \vdots \\ t_n \end{pmatrix}, \quad E_r E_2 t = \begin{pmatrix} t_r \\ -t_1 \\ t_3 \\ \vdots \\ -t_2 \\ \vdots \\ t_n \end{pmatrix}_r, \cdots,$$

$$E_2 E_r E_2 V_2 E_2 E_r E_2 t = \begin{pmatrix} t_1 + t_r \\ t_2 \\ \vdots \\ t_n \end{pmatrix}.$$

但

$$V_r t = \begin{pmatrix} t_1 + t_r \\ t_2 \\ \vdots \\ t_n \end{pmatrix},$$

故得 (5) 式.

例 3. 若 $i \neq s$，命 $y_i = x_i$，而 $y_s = x_s + x_r$ $(r \neq s)$. 此亦為一模變換，其所對應之模方陣即為將 I 之第 s 行加到第 r 行去後所得之方陣(或第 r 列加到第 s 列去後所得之方陣)，以 V_{rs} 記之：

$$V_{rs} = \begin{array}{cc} \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & \cdots & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} & \begin{matrix} \\ \\ r \\ \\ s \\ \\ \\ \end{matrix} \\ \begin{matrix} & & & r & & s & & \end{matrix} & \end{array} \tag{6}$$

當 $s > 1$ 時，$V_{rs} = E_r^{-1} V_s E_r$，而 $V_{r1} = E_r^{-1} V_r^{-1} E_r$. 故 V_{rs} 亦可由 V_2 及 $E_2, \cdots, E_n$ 之乘方乘積表出之.

V_{rs} $(1 \leqslant r \leqslant n,\ 1 \leqslant s \leqslant n,\ r \neq s)$ 及其所有的乘方乘積成一羣，吾人以 $\mathfrak{M}_n$ 記之. 由定理 1.1 的附註，知由 $V_{21} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ 及 $V_{12} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 所演出的羣

$\mathfrak{M}_2$，即爲所有二行二列的正模方陣所成之羣．今往證明對 n 行 n 列正模方陣亦有此定理，即

定理 1. $\mathfrak{M}_n$ 即爲所有 n 行 n 列正模方陣所成之羣．

顯然 $\mathfrak{M}_n$ 中之任一方陣爲正模方陣，故祇需證明任一正模方陣在 $\mathfrak{M}_n$ 中，亦即證明任一正模方陣皆可表爲諸 V_{rs} 之乘方乘積即可．爲此先證下之諸定理．

定理 2. 若 $(x_1, \cdots, x_n) = d$，則有 $U \in \mathfrak{M}_n$，使

$$(x_1, \cdots, x_n)\, U = (d, 0, \cdots, 0)\,.$$

證：當 $n = 2$ 時，若 $(x_1, x_2) = d$，則有二整數 r, s 使

$$r x_1 + s x_2 = d, \qquad (r, s) = 1\,.$$

取 $u = -\frac{x_2}{d}$，$v = \frac{x_1}{d}$，則

$$v x_2 + u x_1 = 0\,,$$

$$v r - u s = 1\,.$$

由是得

$$(x_1, x_2)\begin{pmatrix} r & u \\ s & v \end{pmatrix} = (d, 0),$$

而 $P = \begin{pmatrix} r & u \\ s & v \end{pmatrix}$ 乃一正模方陣、且由定理 1.1 的附註知 $P \in \mathfrak{M}_2$．故當 $n = 2$ 時定理眞實．

今用歸納法．命 $(x_{n-1}, x_n) = d_1$，則有一 $P \in \mathfrak{M}_2$，使

$$(x_{n-1}, x_n)\ P = (d_1, 0)\,.$$

命

$$V^{(n)} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & r & u \\ 0 & 0 & \cdots & s & v \end{pmatrix} = \begin{pmatrix} I^{(n-2)} & 0 \\ 0 & P \end{pmatrix},$$

易知 $V^{(n)} \in \mathfrak{M}_n$，而

$$(x_1, \cdots, x_n)\ V^{(n)} = (x_1, \cdots, x_{n-2}, d_1, 0)\,.$$

由歸納法之假定，知有 $V^{(n-1)} \in \mathfrak{M}_{n-1}$，使

$$(x_1, \cdots, x_{n-2}, d_1)\ V^{(n-1)} = (d, 0, \cdots, 0)\,,$$

於是命

$$V_1^{(n)} = \begin{pmatrix} V^{(n-1)} & 0 \\ 0 & 1 \end{pmatrix},$$

卽得

$$(x_1, \cdots, x_n)\, V^{(n)}\, V_1^{(n)} = (d, 0, \cdots, 0).$$

命 $U = V^{(n)} V_1^{(n)}$，易知 $U \in \mathfrak{M}_n$. 故得定理。

定理 3. 若 $(a_{11}, a_{12}, \cdots, a_{1n}) = d$，則有 $\mathfrak{M}_n$ 中之一方陣以 $\left(\frac{a_{11}}{d}, \frac{a_{12}}{d}, \cdots, \frac{a_{1n}}{d}\right)$ 爲其第一行.

證： 由定理 2 已知有 $\mathfrak{M}_n$ 中之一方陣 U，使

$$(a_{11}, a_{12}, \cdots, a_{1n})\, U = (d, 0, \cdots, 0),$$

而 U^{-1} 卽合所求.

定理 1 的證明： 用歸納法. 當 $n=2$ 時，由定理 1.1 的附註知本定理眞實. 今設

$$A = \begin{pmatrix} a_{11} & a_{12} \cdots & a_{1n} \\ a_{21} & a_{22} \cdots & a_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{n1} & a_{n2} \cdots & a_{nn} \end{pmatrix}$$

爲任一正模方陣. 易知 $(a_{11}, a_{12}, \cdots, a_{1n}) = 1$. A 乘以定理 3 證明中之 U，卽得

$$AU = \begin{pmatrix} 1 & 0 & \cdots 0 \\ a'_{21} & a'_{22} \cdots & a'_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a'_{n1} & a'_{n2} \cdots & a'_{nn} \end{pmatrix}.$$

方陣

$$V = \begin{pmatrix} 1 & 0 & 0 \cdots 0 \\ -a'_{21} & 1 & 0 \cdots 0 \\ -a'_{31} & 0 & 1 \cdots 0 \\ \cdots\cdots & \cdots & \cdots\cdots \\ -a'_{n1} & 0 & 0 \cdots 1 \end{pmatrix}$$

在 $\mathfrak{M}_n$ 中，而

$$VAU = \begin{pmatrix} 1 & 0 & 0 & \cdots 0 \\ 0 & a'_{22} & a'_{23} \cdots & a'_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ 0 & a'_{n2} & a'_{n3} \cdots & a'_{nn} \end{pmatrix}. \tag{7}$$

由歸納法之假定，$\begin{pmatrix} a'_{22} & a'_{23} & \cdots & a'_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a'_{n2} & a'_{n3} & \cdots & a'_{nn} \end{pmatrix}$ 在 $\mathfrak{M}_{n-1}$ 中，因而 $\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & a'_{22} & a'_{23} & \cdots & a'_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & a'_{n2} & a'_{n3} & \cdots & a'_{nn} \end{pmatrix}$ 在 $\mathfrak{M}_n$ 中. 故由 (7) 式卽得定理.

§3. 模方陣之演出元素.

在 §1 中我們已經證明：任一二行二列的正模方陣可由二方陣 $V_{21}=\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $V_{12}=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 之乘方乘積表出. 今往討論一般之情況，卽問任一 n 行 n 列的正模方陣可由那幾個方陣的乘方乘積表出？也就是問 $\mathfrak{M}_n$ 可由那幾個方陣演出？

由定義，知 $\mathfrak{M}_n$ 中之任一方陣是諸 V_{rs} 的乘方乘積，又由上節知 V_{rs} 可由 n 個方陣

$$E_2=\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ -1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}, \cdots, E_n=\begin{pmatrix} 0 & 0 & 0 & \cdots & 1 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ -1 & 0 & 0 & \cdots & 0 \end{pmatrix}, V_2=\begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

之乘方乘積表出，故 $\mathfrak{M}_n$ 可由 n 個方陣 $E_2, E_3, \cdots, E_n, V_2$ 演出之.

命

$$U_1=\begin{pmatrix} 0 & 0 & \cdots & 0 & (-1)^{n-1} \\ 1 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix},$$

則易證 $E_2, E_3, \cdots, E_n$ 都可由 U_1 及 E_2 的乘方乘積表出. 實際上，我們有

$$\begin{aligned} E_r &= (E_2 U_1)^{r-2} E_2 (E_2 U_1)^{n-r+1}, && \text{若 } n \text{ 爲偶數}, \\ E_r &= (E_2^{-1} U_1)^{r-2} E_2 (E_2^{-1} U_1)^{n-r+1}, && \text{若 } n \text{ 爲奇數}, r \text{ 爲偶數}, \qquad (1) \\ E_r &= (E_2^{-1} U_1)^{r-2} E_2^{-1} (E_2^{-1} U_1)^{n-r+1}, && \text{若 } n \text{ 爲奇數}, r \text{ 爲奇數}. \end{aligned}$$

此諸式之證明可仿 (2.5) 式之證明行之.

故 $\mathfrak{M}_n$ 可由三方陣 U_1, V_2, E_2 演出之. 如命

$$U^*=\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix},$$

易見

$$E_2 = U^{*-1} V_2 U^{*^{-1}}.$$

故 $\mathfrak{M}_n$ 亦可由三方陣

$$U_1 = \begin{pmatrix} 0 & 0 & \cdots & 0 & (-1)^{n-1} \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \quad U_2 = V_2 = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}, \quad U^* = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \tag{2}$$

演出之.

在 $n=2$ 的情況, $\mathfrak{M}_2$ 可由二方陣 $U_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ 及 $U_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 演出之. 於是就產生一問題, 卽 $\mathfrak{M}_n (n \geqslant 3)$ 是否也可由 U_1, U_2 二方陣演出, 亦卽 U^* 是否可由 U_1, U_2 的乘方乘積表出. 今先考察 $n=3$ 及 4 之情況.

1) $n=3$. 此時

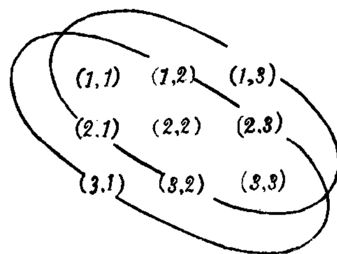
$$U_1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad U_2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad U^* = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

爲了方便起見, "(i, j) 位置" 卽表示第 i 行第 j 列處之位置. 從

$$S = U_1 U_2 U_1^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad T = U_1^2 U_2 (U_1^{-1})^2 = U_1^{-1} U_2 U_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix},$$

$$U_1^3 U_2 (U_1^{-1})^3 = U_2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

可知在 U_2 前面乘以 U_1, 後面乘以 U_1^{-1}, 並連續施行此種手續, 可使 U_2 之對角線元素保持不變, 而非對角線上之 1 沿着 (1,2), (2,3), (3,1) 三個位置移動. 同樣地 (3,2), (1,3), (2,1) 三位置上的元素也在一條軌道上移動, 如右圖所示.



所以要在 (2,1) 位置產生 1, 須先在 (1,3) 或 (3,2) 位置處產生 1. 在 T 的前面乘以 U_2^{-1}, 後面乘以 U_2, 可使 (3,2) 位置產生 1. 卽

$$U_2^{-1}\,T\,U_2=\begin{pmatrix}1&0&0\\0&1&0\\1&1&1\end{pmatrix}.$$

利用前面乘 U_1^{-1}，後面乘 U_1 之手續，可使 $U_2^{-1}\ T\ U_2$ 在 (3,2) 位置之 1 移至 (2,1) 位置，卽

$$W=U_1^{-1}\,U_2^{-1}\,T\,U_2\,U_1=\begin{pmatrix}1&0&0\\1&1&1\\0&0&1\end{pmatrix}.$$

於是只要能消去 (2,3) 位置之 1 卽得 U^*，而此可由前面乘以 S^{-1} 來實現，卽

$$S^{-1}\,W=\begin{pmatrix}1&0&0\\1&1&0\\0&0&1\end{pmatrix}=U^*.$$

故在 $n=3$ 之情況，有

$$U^*=U_1\,U_2^{-1}\,U_1\,U_2^{-1}\,U_1^{-1}\,U_2\,U_1\,U_2\,U_1. \tag{3}$$

2) $n=4$. 此時

$$U_1=\begin{pmatrix}0&0&0&-1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{pmatrix},\quad U_2=\begin{pmatrix}1&1&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix},\quad U^*=\begin{pmatrix}1&0&0&0\\1&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}.$$

與 $n=3$ 時一樣，我們先從

$$T=U_1^{-1}\,U_2\,U_1=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\-1&0&0&1\end{pmatrix}$$

出發. 在 T 的前面乘以 U_2^{-1}，後面乘以 U_2，可在 (4,2) 位置產生 -1，卽

$$U_2^{-1}\,T\,U_2=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\-1&-1&0&1\end{pmatrix}.$$

又經過前面乘 U_1^{-1}，後面乘 U_1 之手續，可將 (4,2) 位置之 -1 移至 (3,1) 位置，卽

$$U_1^{-1}(U_2^{-1}\,T\,U_2)\,U_1=\begin{pmatrix}1&0&0&0\\0&1&0&0\\-1&0&1&1\\0&0&0&1\end{pmatrix}. \tag{4}$$

再施行前面乘 U_2^{-1}，後面乘 U_2 之手續，可使 (3,2) 位置產生 -1，即

$$U_2^{-1}(U_1^{-1}U_2^{-1}TU_2U_1)U_2=\begin{pmatrix}1&0&0&0\\0&1&0&0\\-1&-1&1&1\\0&0&0&1\end{pmatrix}.$$

於是再施行前面乘 U_1^{-1}，後面乘 U_1 之手續，可使 (3,2) 位置之 -1 移至 (2,1) 位置，即

$$W=U_1^{-1}(U_2^{-1}U_1^{-1}U_2^{-1}TU_2U_1U_2)U_1=\begin{pmatrix}1&0&0&0\\-1&1&1&1\\0&0&1&0\\0&0&0&1\end{pmatrix}.$$

至此，對角線以下之形式已經和 U^{*-1} 對角線以下之形式一致，問題在於消去對角線以上之 1.

由 (4) 式可得

$$S=U_1^{-1}(U_1^{-1}U_2^{-1}TU_2U_1)U_1=\begin{pmatrix}1&0&0&0\\0&1&1&1\\0&0&1&0\\0&0&0&1\end{pmatrix},$$

於是立得

$$S^{-1}W=\begin{pmatrix}1&0&0&0\\-1&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}=U^{*-1}.$$

故在 $n=4$ 之情况，有

$$U^{*-1}=U_1^{-1}U_1^{-1}U_2^{-1}U_1^{-1}U_2^{-1}U_1U_2U_1U_1U_1^{-1}U_2^{-1}U_1^{-1}U_2^{-1}U_1^{-1}\cdot$$
$$\cdot U_2U_1U_2U_1U_2U_1. \tag{5}$$

若命 $U=U_2U_1$，則由 (3) 及 (5) 得

$$U^*=U_1^{-1}U^{-1}U_1U_1U^{-1}U_1^{-1}U^2 \qquad (n=3).$$
$$U^{*-1}=U_1^{-1}(U^{-1})^2U_1UU_1(U^{-1})^2U_1^{-1}U^3 \qquad (n=4). \tag{6}$$

一般地可以證明

$$U^{*(-1)^{n-1}}=U_1^{-1}(U^{-1})^{n-2}U_1U^{n-3}U_1(U^{-1})^{n-2}U_1^{-1}U^{n-1} \tag{7}$$

此式之證明讀者可仿 (2.5) 式之證明方法行之．故得

定理 1. 正模方陣所成之羣 $\mathfrak{M}_n$ 可由二方陣

$$U_1=\begin{pmatrix} 0 & 0 & \cdots & 0 & (-1)^{n-1} \\ 1 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \quad U_2=\begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

演出之. 換言之,任一正模方陣可以表爲 U_1 及 U_2 之乘方乘積.

任一模方陣若非正模方陣,則以

$$U_3=\begin{pmatrix} -1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

乘之卽成正模方陣. 故得

定理 2. 模方陣全體所成之羣可由 U_1, U_2 及 U_3 三方陣演出之;換言之,任一模方陣可由 U_1, U_2 及 U_3 之乘方乘積表出之.

§4. 左結合.

定義 1. 若有一模方陣 U 使二方陣 A 與 B 之間有下之關係:

$$A=UB,$$

則謂方陣 B 左結合於方陣 A, 並以 $A\overset{L}{=}B$ 記之.

此左結合關係顯然也有反身,對稱,傳遞三性質.

定理 1. 任一方陣必左結合於一如下形式的方陣

$$\begin{pmatrix} b_{11} & 0 & 0 & \cdots\cdots & 0 & 0 \\ b_{21} & b_{22} & 0 & \cdots\cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ b_{n-1,1} & b_{n-1,2} & b_{n-1,3} & \cdots & b_{n-1,n-1} & 0 \\ b_{n1} & b_{n2} & b_{n3} & \cdots\cdots & b_{n,n-1} & b_{nn} \end{pmatrix}, \tag{1}$$

其中 $b_{\nu\nu}\geqslant 0$. 且若 $b_{\nu\nu}>0$, 則 $0\leqslant b_{i\nu}<b_{\nu\nu}$ $(i>\nu)$.

證: 已知當 $n=2$ 時定理眞實 (定理 1.3). 今用歸納法.

命

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

爲任一方陣. 若 A 之最後一列中至少有一元素不爲 0, 則命 $(a_{1n}, a_{2n}, \cdots,$

$a_{nn}) = b_{nn}$, 有整數 $b_1, b_2, \cdots, b_n$ 使

$$b_1 a_{1n} + b_2 a_{2n} + \cdots + b_n a_{nn} = b_{nn}, \qquad (b_1, b_2, \cdots, b_n) = 1.$$

由定理 2.3, 知有一模方陣 V 以 $(b_1, b_2, \cdots, b_n)$ 爲其第一行. 將 V 之第一行與第 n 行互換後仍得一模方陣 U, 而以 $(b_1, b_2, \cdots, b_n)$ 爲其第 n 行. 因得

$$A \overset{L}{=} UA = \begin{pmatrix} a'_{11} & a'_{12} & \cdots & a'_{1n} \\ a'_{21} & a'_{22} & \cdots & a'_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a'_{n1} & a'_{n2} & \cdots & b_{nn} \end{pmatrix}.$$

易見 $a'_{1n}, \cdots, a'_{n-1,n}$ 皆爲 $a_{1n}, a_{2n}, \cdots, a_{nn}$ 的線性組合, 因而皆能被 b_{nn} 除盡. 於是得

$$A \overset{L}{=} \begin{pmatrix} 1 & 0 & \cdots & 0 & -\frac{a'_{1n}}{b_{nn}} \\ 0 & 1 & \cdots & 0 & -\frac{a'_{2n}}{b_{nn}} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} a'_{11} & a'_{12} & \cdots & a'_{1n} \\ a'_{21} & a'_{22} & \cdots & a'_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a'_{n1} & a'_{n2} & \cdots & b_{nn} \end{pmatrix} = \begin{pmatrix} a''_{11} & \cdots & a''_{1,n-1} & 0 \\ a''_{21} & \cdots & a''_{2,n-1} & 0 \\ \cdots & \cdots & \cdots & \cdots \\ a''_{n-1,1} & \cdots & a''_{n-1,n-1} & 0 \\ a''_{n1} & \cdots & a''_{n,n-1} & b_{nn} \end{pmatrix}. \quad (2)$$

當 A 之最後一列元素全爲 0 時,亦有上式,不過此時 $b_{nn} = 0$. 於是由歸納法之假設可知

$$A \overset{L}{=} \begin{pmatrix} b_{11} & 0 & \cdots 0 & 0 \\ b_{21} & b_{22} & \cdots 0 & 0 \\ \cdots & \cdots & \cdots & \cdots \\ b_{n-1,1} & b_{n-1,2} & \cdots b_{n-1,n-1} & 0 \\ b'_{n1} & b'_{n2} & \cdots b'_{n,n-1} & b_{nn} \end{pmatrix},$$

其中 $b_{\nu\nu} \geqslant 0$, $b_{i\nu} = 0$ $(i<\nu)$, 且若 $b_{\nu\nu}>0$, 則 $0 \leqslant b_{i\nu} < b_{\nu\nu}$ $(1 \leqslant \nu < i \leqslant n-1)$

若 $b_{n-1\ n-1} > 0$, 則有整數 q_{n-1} 存在,使

$$0 \leqslant q_{n-1} b_{n-1,n-1} + b'_{n,n-1} < b_{n-1,n-1}.$$

故

$$A \overset{L}{=} \begin{pmatrix} b_{11} & 0 & \cdots 0 & 0 \\ b_{21} & b_{22} & \cdots 0 & 0 \\ \cdots & \cdots & \cdots & \cdots \\ b_{n-1,1} & b_{n-1,2} & \cdots b_{n-1,n-1} & 0 \\ b''_{n1} & b''_{n2} & \cdots b''_{n,n-1} & b_{nn} \end{pmatrix},$$

其中 $b''_{ni} = q_{n-1} b_{n-1,i} + b'_{ni}$ $(1 \leqslant i \leqslant n-1)$, $0 \leqslant b''_{n,n-1} < b_{n-1,n-1}$.

續行此法卽得定理.

定義 2. 形如 (1) 的方陣稱為左結合標準形式.

習題. 證明非奇異方陣之左結合標準形式是唯一的.

§5. 不變因子. 初等因子.

定義 1. 對二矩陣 $A(=A^{(m,n)})$, $B(=B^{(m,n)})$ 若有二模方陣 $U(=U^{(m)})$, $V(=V^{(n)})$ 使

$$A=UBV,$$

則 A 與 B 謂之相似,以 $A\sim B$ 記之.

顯然相似關係也有反身,對稱及傳遞三性質.

定理 1. 任一矩陣 $A(=A^{(m,n)})$ 必與一形如

$$\begin{pmatrix} d_1 & 0 & 0 & \cdots & 0 & 0\cdots 0 \\ 0 & d_1 d_2 & 0 & \cdots & 0 & 0\cdots 0 \\ 0 & 0 & d_1d_2d_3 & \cdots & 0 & 0\cdots 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & d_1d_2\cdots d_m & 0\cdots 0 \end{pmatrix} \quad (m\leqslant n) \tag{1}$$

或

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_1 d_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & d_1d_2\cdots d_n \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \quad (m\geqslant n) \tag{2}$$

之矩陣相似,其中 $d_i\geqslant 0$.

證: 設

$$A=(a_{11},a_{12},\cdots,a_{1k})$$

為一 1 行 k 列的矩陣,其中 k 為任意的正整數 $(k>1)$, 則由定理 2.2, 知有一正模方陣 U 使

$$AU=(d,0,\cdots,0).$$

故定理成立. 又由於

$$U'\begin{pmatrix} a_{11} \\ a_{12} \\ \vdots \\ a_{1k} \end{pmatrix}=\begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

此處 U' 表示把 U 之行列互換後所得之方陣,可知定理對 k 行 1 列的矩陣也真實.

今於行數上行歸納法. 給與一矩陣 A. 若 $A=0$, 則定理顯然. 若 $A\neq 0$, 則不妨設 $a_{11}\neq 0$, 且亦不妨設 $a_{11}>0$. 今先證 A 必與一如下形式之矩陣相似:

$$A\sim A_1=\begin{pmatrix} a'_{11} & a'_{12} & \cdots & a'_{1n} \\ a'_{21} & a'_{22} & \cdots & a'_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a'_{m1} & a'_{m2} & \cdots & a'_{mn} \end{pmatrix},\quad a'_{11}\mid a'_{ij}\quad (1\leqslant i\leqslant m,\ 1\leqslant j\leqslant n).$$

當 $a_{11}=1$ 時,此乃顯然. 當 $a_{11}>1$ 時,若 $a_{11}\nmid a_{i_0j_0}$, 則經過行的互換和列的互換可以把 $a_{i_0j_0}$ 搬至 a_{12}, a_{21}, a_{22} 三元素之位置. 於是用定理 1.5 的證明方法,可使爲首之元素變爲小於 a_{11} 之正整數,故由歸納法卽得所云.

由

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ -\frac{a'_{21}}{a'_{11}} & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ -\frac{a'_{m1}}{a'_{11}} & 0 & \cdots & 1 \end{pmatrix}\begin{pmatrix} a'_{11} & a'_{12} & \cdots & a'_{1n} \\ a'_{21} & a'_{22} & \cdots & a'_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a'_{m1} & a'_{m2} & \cdots & a'_{mn} \end{pmatrix}\begin{pmatrix} 1 & -\frac{a'_{12}}{a'_{11}} & \cdots & -\frac{a'_{1n}}{a'_{11}} \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}=$$

$$=\begin{pmatrix} a'_{11} & 0 & \cdots & 0 \\ 0 & a''_{22} & \cdots & a''_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & a''_{m2} & \cdots & a''_{mn} \end{pmatrix},$$

可知

$$A\sim\begin{pmatrix} a'_{11} & 0 & \cdots & 0 \\ 0 & a''_{22} & \cdots & a''_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & a''_{m2} & \cdots & a''_{mn} \end{pmatrix}.$$

於是由歸納法之假設,可知

$$A\sim\begin{pmatrix} a'_{11} & 0 & 0\cdots & 0 & 0\cdots 0 \\ 0 & d'_2 & 0\cdots & 0 & 0\cdots 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0\cdots d'_2 & \cdots d'_m & 0\cdots 0 \end{pmatrix}\quad (m\leqslant n) \tag{4}$$

或

$$A\sim\begin{pmatrix} a'_{11} & 0 & \cdots & 0 \\ 0 & d'_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots d'_2 & \cdots d'_n \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}\quad (m\geqslant n). \tag{5}$$

由於 $a'_{11}|a'_{ij}$, 而 d'_2 是 A_1 中某些元素的線性組合,所以 $a'_{11}|d'_2$. 如命 $a'_{11}=d_1$, $d'_2=d_1d_2$, $d'_3=d_3$, $d'_4=d_4$, $\cdots$. 則由 (4) 及 (5) 卽得定理.

定義 2. 形如 (1) 或 (2) 的矩陣稱爲相似標準形式.

在定理 1 的證明過程中,所行的手續祗是行的互換或列的互換; 一行乘一整數加到另一行,或一列乘一整數加到另一列去; 以 -1 乘一行或一列. 如此數種手續稱爲初等變換. 故定理 1 可以改述爲: 經初等變換可將一矩陣化爲相似標準形式.

一矩陣的兩行 (或列) 互換後,或以 -1 乘以一行 (或列) 後,所得矩陣之任一 i 行 i 列子行列式,或與原矩陣之一 i 行 i 列子行列式相同, 或僅相差一符號; 又若以一矩陣的一行 (或列) 乘一整數加到另一行 (或列) 去,則所得矩陣之任一 i 行 i 列子行列式,或爲原矩陣之一 i 行 i 列子行列式,或爲一 i 行 i 列子行列式加另一 i 行 i 列子行列式的整數倍. 故經初等變換後,一矩陣之所有 i 行 i 列子行列式的最大公因數不變. 故得

定理 2. 若 $A\sim B$, 則 A 內所有 i 行 i 列子行列式的最大公因數與 B 內所有 i 行 i 列子行列式的最大公因數相等.

同時由 (1) 及 (2),知

$$h_i=d_1\cdot d_1d_2\cdots d_1\cdots d_i$$

卽爲 A 中諸 i 行 i 列子行列式的最大公因數. 故得

定理 3. 任一矩陣的相似標準形式是唯一的.

定義 3. 在矩陣 A 的相似標準形式 (1) 或 (2) 中,對角線上不爲零的元素

$$d_1,\ d_1d_2,\cdots,d_1\cdots d_k\quad (k\leqslant\min(m,n)),$$

分別稱爲 A 的 1 次, 2 次, $\cdots$, k 次不變因子. k 稱爲矩陣 A 的秩. 不變因子的標準分解式

$$d_1\cdots d_i=p_1^{e_{i1}}\cdots p_{l_i}^{e_{il_i}}\quad (e_{ij}>0,\ \ 1\leqslant i\leqslant k,\ \ l_{i-1}\leqslant l_i)$$

中,所有的素數冪 $p_j^{e_{ij}}$ 都稱爲 A 的初等因子.

易知初等因子的指數間有下之關係:

$$e_{k,j}\geqslant e_{k-1,j}\geqslant e_{k-2,j}\geqslant\cdots\quad (1\leqslant j\leqslant l).$$

由定義易知:二矩陣如有相同的不變因子,則有相同的秩和相同的初等因子;

反之,如有相同的秩和初等因子,則有相同的不變因子. 故得:

定理 4. 二 $m\times n$ 矩陣 A 與 B 相似的充要條件是 A 與 B 有相同的秩和相同的初等因子.

§6. 應用.

研究整係數線性方程組

$$y_i=\sum_{j=1}^{n}x_j a_{ji}\qquad(1\leqslant i\leqslant m,\quad n\geqslant m),\tag{1}$$

之整數解,其中 y_i 是已給的整數,卽研究

$$y=xA,\quad y=(y_1,\cdots,y_m),\quad x=(x_1,\cdots,x_n),\quad A=\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1m}\\a_{21}&a_{22}&\cdots&a_{2m}\\\cdots&\cdots&\cdots&\cdots\\a_{n1}&a_{n2}&\cdots&a_{nm}\end{pmatrix}\tag{2}$$

之整數解.

由上節知有二模方陣 $U(=U^{(n)})$ 及 $V(=V^{(m)})$, 使

$$UAV=\begin{pmatrix}d_1&0&\cdots&0\\0&d_1d_2&\cdots&0\\\cdots&\cdots&\cdots&\cdots\\0&0&\cdots&d_1\cdots d_m\\0&0&\cdots&0\\\cdots&\cdots&\cdots&\cdots\\0&0&\cdots&0\end{pmatrix}=D.\tag{3}$$

於是命

$$yV=y^*=(y_1',\cdots,y_m'),\quad xU^{-1}=x^*=(x_1',\cdots,x_n'),$$

則由 (2) 卽得

$$y^*=x^*D.\tag{4}$$

由 (4),

$$y_i'=d_1\cdots d_i x_i'\quad(1\leqslant i\leqslant m).\tag{5}$$

(1) 式有解的充要條件是 (5) 式有解. 如 $d_1\cdots d_k\neq0$, $d_{k+1}=0$, 則 (5) 式有解之充要條件是

$$d_1\cdots d_i\mid y_i'\quad(1\leqslant i\leqslant k),\quad y_{k+1}'=\cdots=y_m'=0.\tag{6}$$

由 (3) 可知

$$\begin{pmatrix}U&0\\0&1\end{pmatrix}\begin{pmatrix}A\\y\end{pmatrix}V=\begin{pmatrix}D\\y^*\end{pmatrix}.\tag{7}$$

今若 (6) 式成立,則由 (7),

$$\begin{pmatrix} A \\ y \end{pmatrix} \sim \begin{pmatrix} D \\ 0 \end{pmatrix}; \tag{8}$$

反之,若 (8) 式成立,則得

$$\begin{pmatrix} D \\ y^* \end{pmatrix} \sim \begin{pmatrix} D \\ 0 \end{pmatrix}.$$

由定理 5.2, 卽得

$$d_1 \mid y'_1, \quad d_1 d_2 \mid y'_2, \quad \cdots, \quad d_1 \cdots d_k \mid y'_k, \quad y'_{k+1} = \cdots = y'_m = 0,$$

此卽 (6) 式. 故 (1) 式有解之充要條件是 (8) 式成立. 卽:

定理. 方程組 (1) 有解的必要且充分條件是二矩陣 A 及 $\begin{pmatrix} A \\ y \end{pmatrix}$ 有相同的不變因子.

若 (5) 式成立,則可得

$$x'_1 = \frac{y'_1}{d_1}, \quad x'_2 = \frac{y'_2}{d_1 d_2}, \cdots, \quad x'_k = \frac{y'_k}{d_1 \cdots d_k}. \tag{9}$$

卽 $x'_1, x'_2, \cdots, x'_k$ 都唯一地決定,而 $x'_{k+1}, \cdots, x'_n$ 可以是任意的整數. 因此如命 $t_1, \cdots, t_{n-k}$ 表 $n-k$ 個整襄變數,則有

$$\begin{aligned} x_i &= \sum_{j=1}^{k} x'_j u_{ji} + \sum_{l=1}^{n-k} t_l u_{k+l,i} \\ &= x_i^{(0)} + \sum_{l=1}^{n-k} t_l u_{k+l,i} \qquad (1 \leqslant i \leqslant n), \end{aligned} \tag{10}$$

此處 $x_1^{(0)}, \cdots, x_n^{(0)}$ 卽爲當 $t_1 = \cdots = t_{n-k} = 0$ 時 (1) 式的一組解.

§7. 因子分解. 標準素方陣.

定義 1. 對二方陣 A, B, 如有一方陣 C 使 $A = CB$, 則稱 B 爲 A 的右因子,或 B 右除盡 A, 並逕以 $B|A$ 記之.

顯然有 (i) $A|A$; (ii) 若 $A|B$, $B|C$ 則 $A|C$.

左因子與左除盡的定義,可同樣得出.

定義 2. 設 A 非奇異方陣,且亦非模方陣. 若對 A 的任何分解式 $A=BC$, 常得出 B 或 C 是模方陣,則稱 A 爲不可分解方陣或素方陣. 不然,稱 A 爲複合方陣.

設 A 是非奇異方陣,則由定理 5.1 可知有二模方陣 U 及 V 使

$$A=U\left[d_1, d_1d_2, \cdots, d_1\cdots d_n\right] V. \tag{1}$$

極易把 $[d_1, d_1 d_2, \cdots, d_1\cdots d_n]$ 分解爲素方陣，且可更確切些說，其因子之形式爲 $P=[1,\cdots,1, p, 1,\cdots,1]$，此處 p 爲素數，且因子之個數等於 $d_1\cdot d_1d_2\cdot\cdots\cdot d_1d_2\cdots d_n$ 之素因子數. 故有

$$A=U P_1 P_2\cdots P_s V, \qquad P=[1,\cdots,1, p, 1,\cdots,1]. \tag{2}$$

其中任二 P 是可以交換的. 由此立得:

定理 1. 一方陣爲一素方陣之充分且必要條件是其行列式爲素數.

定理 2. 任一複合方陣可以分解爲有限多個素方陣之積，且其因子數等於其行列式之素因子數.

此種分解法是否唯一，其回答是否定的. 因爲於任二因子 P_i, P_{i+1} 間可以插入 WW^{-1} (W 是模方陣)，P_iW 及 $W^{-1}P_{i+1}$ 一般與 P_i 及 P_{i+1} 不相同. 但若對因子之形式加以適當的限制，仍可得類似的定理.

定義 3. 若一素方陣可以表成爲 $U^{-1}[1,\cdots,1, p]\ U$ 之形式，則此素方陣稱爲標準素方陣，此處 U 是模方陣.

顯然任一素方陣必左結合於一標準素方陣.

今將 (2) 式改寫爲如下之形式:

$$A=UV(V^{-1}P_1V)(V^{-1}P_2V)\cdots(V^{-1}P_sV), \tag{3}$$

其中任二 $V^{-1}PV$ 也是可以交換的，且皆爲標準素方陣，故得:

定理 3. 任一複合方陣必左結合於有限多個可交換的標準素方陣之積.

定義 4. A 之標準分解式乃指下式而言:

$$A=W(V^{-1}P_1V)(V^{-1}P_2V)\cdots(V^{-1}P_sV), \tag{4}$$

此處 W 和 V 是模方陣，$P_1,\cdots,P_s$ 之形狀與(2)式中相同. 顯然，若不計次序，$P_1,\cdots,P_s$ 由 A 唯一決定.

在證明類似於唯一性的定理之前，先需引進以下之定義:

定義 5. 對一非奇異方陣 A，適合於

$$AUA_0\equiv 0 \qquad (\mathrm{mod}\ |A|)$$

之模方陣 U 稱爲 A 之伴隨模方陣，此處 A_0 表 A 之伴隨方陣，$|A|$ 表 A 的

行列式的絕對值.

既然 AUA_0 之元素皆爲 $|A|$ 之倍數,則得 $\frac{1}{|A|}AUA_0$ 是一整數元素的方陣. 取行列式可見此乃一模方陣.

定理 4. A 之伴隨模方陣成一羣.

證 若 U,V 是 A 之伴隨模方陣,由於

$$AUA_0AVA_0=\pm|A|\cdot AUVA_0\equiv 0 \pmod{|A|^2},$$

故 UV 爲伴隨模方陣. 又由

$$|A|AIA_0=\pm AUA_0AU^{-1}A_0\equiv 0 \pmod{|A|^2},$$

得

$$\frac{1}{|A|}AUA_0\cdot AU^{-1}A_0\equiv 0 \pmod{|A|},$$

而 $\frac{1}{|A|}AUA_0$ 爲模方陣, 故 U^{-1} 也是伴隨模方陣. 由此可得定理.

定義 6. A 之伴隨模方陣所成之羣稱爲 A 之伴隨模羣.

定理 5. 設

$$A=W_1(V_1^{-1}P_1V_1)(V_1^{-1}P_2V_1)\cdots(V_1^{-1}P_sV_1) \tag{5}$$

爲 A 之另一標準分解式, 則有一 A 之伴隨模方陣 U 存在, 使 $V_1=VU$, $W_1=\frac{1}{\pm|A|}AU^{-1}A_0WU$, 此處之 W 和 V 爲 (4) 式中之模方陣.

證: 由 (4) 與 (5) 可知

$$A=WV^{-1}P_1P_2\cdots P_sV=W_1V_1^{-1}P_1P_2\cdots P_sV_1,$$

故得

$$AV^{-1}V_1=WV^{-1}V_1W_1^{-1}A.$$

由上式易見 $U=V^{-1}V_1$ 爲 A 之伴隨模方陣, 且知

$$\frac{1}{\pm|A|}AUA_0=WUW_1^{-1}.$$

故得定理. 此定理說明 A 之兩標準分解式之間的關係.

關於可交換的標準素方陣, 有以下之二定理:

定理 6. 設 $P=[1,\cdots,1,p]$, $Q=U^{-1}[1,\cdots 1,q]\ U$ 是可交換的二標準素方陣,則 Q 必取如下之形式:

$$Q=\begin{pmatrix} Q_1 & 0\\ 0 & r\end{pmatrix}, \tag{6}$$

其中 $r=q$ 或 1. 且若 $r=q$, 則 $Q_1=I$; 若 $r=1$, 則 Q_1 爲標準素方陣.

證: 命

$$Q=\begin{pmatrix} Q_1 & x \\ y & r \end{pmatrix}, \quad x=\begin{pmatrix} a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}, \quad y=(b_1,\cdots,b_{n-1}).$$

由 $PQ=QP$, 得

$$\begin{pmatrix} Q_1 & x \\ py & pr \end{pmatrix}=\begin{pmatrix} Q_1 & xp \\ y & rp \end{pmatrix}. \tag{7}$$

由此立得 $x=\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$, $y=(0,\cdots,0)$.

又命

$$U=\begin{pmatrix} U_1 & x_1 \\ y_1 & u \end{pmatrix},$$

則從 $UQ=[1,\cdots,1,q]\,U$, 可得

$$\begin{pmatrix} U_1Q_1 & x_1r \\ y_1Q_1 & ur \end{pmatrix}=\begin{pmatrix} U_1 & x_1 \\ qy_1 & qu \end{pmatrix}. \tag{8}$$

若 $u\neq 0$, 則得 $r=q$. 此時由 $x_1r=x_1$, 得 $x_1=\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$,因得 $u=\pm 1$, U_1 是模方陣,故由 $U_1Q_1=U_1$, 卽得 $Q_1=I$.

若 $u=0$, 則 $x_1\neq\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$,故得 $r=1$. 從 $U_1Q_1=U_1$, 因 Q_1 不能等於 I, 故 U_1 是奇異方陣. 由定理 5.1 知存在二模方陣 V_1 及 W_1, 使 $V_1U_1W_1=$ $=[\lambda_1,\cdots,\lambda_{n-2},0]$, $\lambda_i\geqslant 0$. 故若命

$$V=\begin{pmatrix} V_1 & 0 \\ 0 & 1 \end{pmatrix}, \quad W=\begin{pmatrix} W_1 & 0 \\ 0 & 1 \end{pmatrix},$$

則有

$$X=VUW=\begin{pmatrix} V_1U_1W_1 & V_1x_1 \\ y_1W_1 & 0 \end{pmatrix}=\begin{pmatrix} \lambda_1 & 0 & \cdots & 0 & 0 & c_1 \\ 0 & \lambda_2 & \cdots & 0 & 0 & c_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \lambda_{n-2} & 0 & c_{n-2} \\ 0 & 0 & \cdots & 0 & 0 & c_{n-1} \\ d_1 & d_2 & \cdots & d_{n-2} & d_{n-1} & 0 \end{pmatrix}.$$

由於 $|c_{n-1}d_{n-1}\lambda_1\cdots\lambda_{n-2}|=|X|=1$, 故得 $\lambda_1=\cdots=\lambda_{n-2}=1$, $c_{n-1}=\pm 1$, $d_{n-1}=\pm 1$, 此處 $|X|$ 表示 X 之行列式之絕對値.

又命

$$Y=\begin{pmatrix}1 & 0 & \cdots & 0 & \mp c_1 & 0\\ 0 & 1 & \cdots & 0 & \mp c_2 & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & \cdots & 1 & \mp c_{n-2} & 0\\ 0 & 0 & \cdots & 0 & 1 & 0\\ 0 & 0 & \cdots & 0 & 0 & 1\end{pmatrix},\quad Z=\begin{pmatrix}1 & 0 & \cdots & 0 & 0 & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & \cdots & 1 & 0 & 0\\ \mp d_1 & \mp d_2 & \cdots & \mp d_{n-2} & 1 & 0\\ 0 & 0 & \cdots & 0 & 0 & 1\end{pmatrix}=\begin{pmatrix}Z_1 & 0\\ 0 & 1\end{pmatrix},$$

此處矩陣 Y 與 Z 中之負號或正號,分別由 c_{n-1} 與 d_{n-1} 爲 $+1$ 或 -1 而定,則立得

$$YXZ=\begin{pmatrix}1 & 0 & \cdots & 0 & 0 & 0\\ 0 & 1 & \cdots & 0 & 0 & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & \cdots & 1 & 0 & 0\\ 0 & 0 & \cdots & 0 & 0 & c_{n-1}\\ 0 & 0 & \cdots & 0 & d_{n-1} & 0\end{pmatrix}.$$

於是從

$$XW^{-1}QW=VUQW=V[1,\cdots,1,q]UW=[1,\cdots,1,q]X,$$

得

$$YXZZ^{-1}W^{-1}QWZ=Y[1,\cdots,1,q]XZ=[1,\cdots,1,q]YXZ,$$

卽

$$(WZ)^{-1}Q(WZ)=(YXZ)^{-1}[1,\cdots,1,q]YXZ=[1,\cdots,1,q,1].$$

故得

$$(W_1Z_1)^{-1}Q_1(W_1Z_1)=[1,\cdots,1,q].$$

此證明了 Q_1 是標準素方陣.

定理 7. 對任意一組互可交換的標準素方陣 $P_1,\cdots,P_s$, 有一模方陣 U 存在,使 $U^{-1}P_iU$ 皆爲對角線形式.

證: 當 $s=1$ 時定理顯然, 今用歸納法證明此定理. 假定定理當方陣之個數 $<s$ 時已成立.

對 P_s 有模方陣 U_s, 使 $U_s^{-1}P_sU_s=[1,\cdots,1,p_s]$. 命

$$U_s^{-1}P_iU_s=Q_i,\qquad i=1,2,\cdots,s.$$

顯然諸 Q 仍爲互可交換的標準素方陣. 由定理 6 可知

$$Q_i=\begin{pmatrix}Q_i^* & 0\\ 0 & \gamma_i\end{pmatrix},\quad 1\leqslant i\leqslant s,$$

其中 $r_i = p_i$ 或 1. 且若 $r_i = p_i$, 則 $Q_i^* = I$, Q_i 爲對角線形式;若 $r_i = 1$, 則 Q_i^* 是標準素方陣. 由於諸 Q 是互可交換的,故不妨設 $r_1 = r_2 = \cdots = r_t = 1$, $r_{t+1} = p_{t+1}, \cdots, r_s = p_s$, $0 \leqslant t \leqslant s-1$. 若 $t = 0$, 則定理已明. 不然, 則由歸納法之假設, 對諸互可交換的標準素方陣 $Q_1^*, \cdots, Q_t^*$ 有一模方陣 U^*, 使 $U^{*-1} Q_i^* U^* \ (1 \leqslant i \leqslant t)$ 爲對角線形式. 今取

$$U_1 = \begin{pmatrix} U^* & 0 \\ 0 & 1 \end{pmatrix},$$

則 $U_1^{-1} Q_i U_1 \ (1 \leqslant i \leqslant s)$ 皆爲對角線形式. 取 $U = U_s U_1$ 卽得定理.

習題. 取 $A = [d_1, d_1 d_2, \cdots, d_1 \cdots d_n]$ 而研究 A 之伴隨模羣之性質.

§ 8. 最大公約. 最小公倍.

定義 1. 如方陣 D 爲方陣 A 及 B (A 與 B 不同時爲 0) 的右公因子, 且 A, B 之任何右公因子皆爲 D 的右因子,則稱 D 爲 A,B 之右最大公約.

如方陣 A,B 都分別是方陣 M (非 0) 的右因子,且 M 爲任何以 A,B 爲右因子的方陣的右因子,則稱 M 爲 A,B 的左最小公倍.

左最大公約及右最小公倍的定義可同樣得出. 今後僅討論右最大公約及左最小公倍,爲簡單計,並逕稱之爲最大公約及最小公倍.

二方陣 $A = (a_{ij})$ 及 $B = (b_{ij})$ 的和定義爲

$$A + B = (a_{ij} + b_{ij}).$$

定理 1. 不同時爲 0 之二方陣 A,B 必有最大公約 D, 且存在方陣 P 及 Q, 使

$$PA + QB = D.$$

證: 置

$$C = \begin{pmatrix} A \\ B \end{pmatrix}$$

爲一 $2n \times n$ 矩陣. 由定理 5.1, 知有二模方陣 $U(= U^{(2n)})$, $V(= V^{(n)})$, 使

$$UCV = \begin{pmatrix} D_1 \\ O \end{pmatrix}, \qquad D_1 = [d_1, d_1 d_2, \cdots, d_1 d_2 \cdots d_n].$$

記

$$U = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix}, \quad U_{ij} \text{ 爲 } n \times n \text{ 方陣},$$

則由上式得

$$\begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix}\begin{pmatrix} A \\ B \end{pmatrix}=\begin{pmatrix} D_1 \\ O \end{pmatrix}V^{-1}=\begin{pmatrix} D \\ O \end{pmatrix}. \qquad (1)$$

由是得

$$U_{11}A+U_{12}B=D, \qquad (2)$$

故 A,B 之右公因子必爲 D 之右因子.

又如命

$$\begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix}^{-1}=\begin{pmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{pmatrix}, \quad X_{ij} \text{ 爲 } n\times n \text{ 方陣} \qquad (3)$$

則由 (1) 式得

$$\begin{pmatrix} A \\ B \end{pmatrix}=\begin{pmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{pmatrix}\begin{pmatrix} D \\ O \end{pmatrix}.$$

由此得

$$A=X_{11}D, \quad B=X_{21}D,$$

故 D 卽爲 A,B 的最大公約. 再於 (2) 式中令 $U_{11}=P$, $U_{12}=Q$, 卽得定理.

定理 2. 若二方陣 A,B 之一最大公約 D 是非奇異的,則 A,B 之任一最大公約必爲 UD 之形式,此處 U 是模方陣.

證: 設 D_1 是另一最大公約,則由定義,有 $D=RD_1$ 及 $D_1=SD$, 因而得

$$D=RSD.$$

取行列式,易見 R 及 S 是模方陣.

上面已經討論了二方陣的最大公約,今往討論二方陣的最小公倍. 若二方陣都是奇異的,則最小公倍不一定存在. 例如

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ 與 } \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

卽無最小公倍. 因爲以 $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ 爲右因子的方陣必爲 $\begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix}$ 之形式,而以 $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ 爲右因子的方陣必爲 $\begin{pmatrix} a & a \\ c & c \end{pmatrix}$ 之形式. 此兩種形式顯然不能相等,除非 $a=c=0$. 但我們有

定理 3. 二非奇異方陣 A,B 必有一最小公倍 M 存在, 且 M 非奇異的; 而其他之最小公倍皆爲 UM 之形式,此處 U 爲模方陣.

證: 由 (1), 得

$$U_{21} A + U_{22} B = 0.$$

命

$$M = U_{21} A = -U_{22} B,$$

則 M 爲 A,B 之一公倍. 今往證明 M 卽爲 A,B 之最小公倍. 設 M_1 爲 A,B 之另一公倍,則 M, M_1 之最大公約 M_2 亦爲 A,B 之一公倍. 命

$$M = HM_2, \qquad M_2 = KA = LB,$$

則得

$$U_{21} A = HKA, \qquad -U_{22} B = HLB. \tag{4}$$

命 A_0, B_0 分別爲 A,B 之伴隨方陣,則有 $AA_0 = aI$ 及 $BB_0 = bI$, 此處 a,b 分別爲 A,B 之行列式. 由於 A,B 皆非奇異的,卽 $a \neq 0$, $b \neq 0$, 故由 (4) 式可得

$$U_{21} = HK, \quad -U_{22} = HL.$$

於是由 (3) 得

$$I = U_{21} X_{12} + U_{22} X_{22} = H(KX_{12} - LX_{22}),$$

因此 H 爲一模方陣, H^{-1} 存在. 故由

$$M_1 = GM_2 = GH^{-1} M,$$

卽得 M 爲最小公倍.

今往證明 M 爲非奇異方陣. 由最小公倍之定義, 吾人僅須證明 A, B 有非奇異的公倍存在卽可. 由定理 5.1, 知有二模方陣 U_1, V_1, 使

$$U_1 AV_1 = [d_1', d_1' d_2', \cdots, d_1' \cdots d_n'].$$

命

$$M^* = d_1' \cdots d_n' \, U_1 B,$$

顯見 M^* 爲非奇異方陣, 且 $M^* = U_1 BV_1[d_2' \cdots d_n', d_3' \cdots d_n', \cdots, 1]U_1 A$. 此 M^* 卽爲所需.

若 M_3 爲另一最小公倍, 則由定義, 有

$$M = EM_3, \qquad M_3 = FM,$$

因而

$$M = EFM, \qquad I = EF,$$

卽 E, F 爲模方陣. 故得定理.

定理 4. 設 A 爲一方陣,則對任一整數 $m(\neq 0)$, 必存在二方陣 R 及 Q, 使 1) $A = mQ$ 或 2) $A = mQ + R$, 而 $0 < |R| < |m|^n$, 此處 $|R|$ 表示方陣

R 的行列式之絕對值.

證: 由定理 5.1, 知有二模方陣 U 及 V 使

$$A = U[d_1, d_1 d_2, \cdots, d_1 \cdots d_n] V \qquad (d_i \geqslant 0, \quad 1 \leqslant i \leqslant n).$$

有整數 q_i 及 $r_i (>0)$ 使

$$d_1 \cdots d_i = mq_i + r_i, \qquad 0 < r_i \leqslant |m| \qquad (1 \leqslant i \leqslant n).$$

命

$$Q_1 = [q_1, q_2, \cdots, q_n], \qquad R_1 = [r_1, r_2, \cdots, r_n],$$

則得

$$A = U(mQ_1 + R_1) V. \tag{5}$$

若 $r_i = |m|$ $(1 \leqslant i \leqslant n)$, 則 $R_1 = |m| \ I = \pm m I$, 故由 (5) 得

$$A = mU(Q_1 \pm I) V = m Q,$$

此卽 1).

不然, 如有一個 j 使 $0 < r_j < |m|$, 則有 $0 < |R_1| = r_1 r_2 \cdots r_n < |m|^n$, 故由 (5) 得

$$A = m \, UQ_1V + UR_1 V = mQ + R,$$

而 $|R| = |UR_1V| = |R_1|$, 故得 2).

定理 5. 設方陣 B 非奇異的, 則對任一方陣 A, 必存在二方陣 Q 及 C 使 1) $A = QB$ 或 2) $A = QB + C$, 而 $0 < |C| < |B|$.

證: 命 B_0 爲 B 之伴隨方陣, $BB_0 = B_0B = bI$, 此處 b 爲 B 之行列式. 由上定理可知有二方陣 Q 及 R 使

$$AB_0 = bQ \tag{6}$$

或

$$AB_0 = bQ + R, \quad 0 < |R| < |b|^n. \tag{7}$$

於 (6) 式兩邊乘以 B, 並由於 $b \neq 0$, 卽得

$$A = QB,$$

此卽 1). 又由 (7), $R = AB_0 - bQ = AB_0 - QBB_0 = (A - QB) B_0 = = CB_0$. 於是由

$$A = QB + (A - QB) = QB + C$$

及

$$0<|C|=\frac{|R|}{|B_0|}<\frac{|b|^n}{|b|^{n-1}}=|b|=|B|,$$

卽得 2).

§9. **線性模.**

命 $x_1, \cdots, x_n$ 表 n 個未定量,所有的整係數一次式(或稱線性型)

$$y=a_1 x_1+\cdots+a_n x_n$$

成一集合,此集合以 $\mathfrak{O}=\{x_1, \cdots, x_n\}$ 表之.

若 $y'=a_1' x_1+\cdots+a_n' x_n$ 爲另一線性型,則定義

$$y \pm y'=(a_1 \pm a_1') x_1+\cdots+(a_n \pm a_n') x_n.$$

定義 1. $\mathfrak{O}$ 的一個子集合 $\mathfrak{M}$ 如有次之性質則稱爲模: 若 y_1, y_2 在 $\mathfrak{M}$ 中,則 $y_1 \pm y_2$ 亦在 $\mathfrak{M}$ 中.

顯然 $\mathfrak{O}$ 本身是一模. $0, \pm x_1, \pm 2x_1, \cdots$ 所成之集合也成一模. 僅有一元素 $0=0x_1+\cdots+0x_n$ 所成之模不在討論之列.

定義 2. 如模 $\mathfrak{M}$ 中有一組元素 $y_1, \cdots, y_l$, 使 $\mathfrak{M}$ 內任一元素皆可唯一地表成爲

$$b_1 y_1+\cdots+b_l y_l$$

之形式, 其中 $b_1, \cdots, b_l$ 是整數,則 $y_1, \cdots, y_l$ 稱爲 $\mathfrak{M}$ 之底, 數 l 稱爲 $\mathfrak{M}$ 之維數.

由定義易知 $y_1, \cdots, y_l$ 是線性無關的, 卽由 $a_1 y_1+\cdots+a_l y_l=0$ 得出 $a_1=\cdots=a_l=0$.

定理 1. 模必有底,維數 $\leqslant n$.

證: 設 $\mathfrak{M}$ 之所有元素中, $x_{l+1}, \cdots, x_n$ $(l \leqslant n)$ 之係數全爲零.而 x_l 之係數有不爲零者,則易見所有元素之 x_l 之係數成一非零的整數模,其中有一最小正整數,命爲 b_l, 並設對應之線性型爲

$$y_l=b_1 x_1+\cdots+b_l x_l.$$

於是 $\mathfrak{M}$ 中任一元素 y 之 x_l 之係數必爲 b_l 之倍數,故可表爲

$$y=y'+g y_l,$$

此處 g 是一整數, y' 是未定量 $x_1, \cdots, x_{l-1}$ 的線性型. 如此作出之所有 y' 中,

設 $x_{l'+1}, \cdots, x_{l-1}$ $(l' \leqslant l-1)$ 之係數全爲零，而 $x_{l'}$ 的係數有不爲零者，則同上法可得一線性型

$$y_{l'} = b'_1 x_1 + \cdots + b'_{l'} x_{l'} ,$$

其中 $y_{l'}$ 爲諸線性型 y' 中 $x_{l'}$ 之係數爲最小之正整數者．使 $y' = y'' + g' y_{l'}$，其中 g' 爲一整數，y'' 爲 $x_1, \cdots, x_{l'-1}$ 的線性型．續行此法卽得 $\mathfrak{M}$ 的一底 $y_l, y_{l'}, \cdots$，其所含元素之個數 $\leqslant n$．故得定理．

定理 2. 模之維數與底之選擇無關．

證：設 $y_1, \cdots, y_l$ 及 $z_1, \cdots, z_{l'}$ 是模 $\mathfrak{M}$ 的任意二底，今往證明 $l = l'$．若不然，卽 $l \neq l'$，不妨設 $l > l'$．由底之定義，知有整數 a_{ij} 及 b_{ij} 使

$$\begin{pmatrix} y_1 \\ \vdots \\ y_l \end{pmatrix} = \begin{pmatrix} a_{11} \cdots a_{1l'} & 0 \cdots 0 \\ a_{21} \cdots a_{2l'} & 0 \cdots 0 \\ \cdots\cdots\cdots & \cdots\cdots \\ a_{l1} \cdots a_{ll'} & 0 \cdots 0 \end{pmatrix} \begin{pmatrix} z_1 \\ \vdots \\ z_{l'} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

及

$$\begin{pmatrix} z_1 \\ \vdots \\ z_{l'} \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} b_{11} \cdots b_{1l} \\ \cdots\cdots\cdots \\ b_{l'1} \cdots b_{l'l} \\ 0 \cdots 0 \\ \cdots\cdots\cdots \\ 0 \cdots 0 \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_l \end{pmatrix},$$

此處 (a_{ij}) 及 (b_{ij}) 都是 $l \times l$ 方陣．於是得

$$\begin{pmatrix} y_1 \\ \vdots \\ y_l \end{pmatrix} = \begin{pmatrix} a_{11} \cdots a_{1l'} & 0 \cdots 0 \\ a_{21} \cdots a_{2l'} & 0 \cdots 0 \\ \cdots\cdots\cdots & \cdots\cdots \\ a_{l1} \cdots a_{ll'} & 0 \cdots 0 \end{pmatrix} \begin{pmatrix} b_{11} \cdots b_{1l} \\ \cdots\cdots\cdots \\ b_{l'1} \cdots b_{l'l} \\ 0 \cdots 0 \\ \cdots\cdots\cdots \\ 0 \cdots 0 \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_l \end{pmatrix}.$$

但 $y_1, \cdots, y_l$ 是線性無關的，故必須 $(a_{ij}) \cdot (b_{ij}) = I$．因左邊之行列式等於零，故得矛盾．

今後僅討論 n 維模．

設 $y_1, \cdots, y_n$ 爲一 n 維模 $\mathfrak{M}$ 的底，則有

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \cdots a_{1n} \\ a_{21} & a_{22} \cdots a_{2n} \\ \cdots & \cdots \\ a_{n1} & a_{n2} \cdots a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}. \tag{1}$$

故對一 n 維模及其一底 $y_1, \cdots, y_n$ 有一方陣

$$A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} \cdots a_{1n} \\ a_{21} & a_{22} \cdots a_{2n} \\ \cdots & \cdots \\ a_{n1} & a_{n2} \cdots a_{nn} \end{pmatrix} \tag{2}$$

與之對應. 由於 $y_1, \cdots, y_n$ 是線性無關的,故 A 是非奇異的. 反之,對一非奇異方陣 A, 由 (1) 可定出一組線性無關的線性型 $y_1, \cdots, y_n$, 從而可定出一以 $y_1, \cdots, y_n$ 爲底的 n 維模 $\mathfrak{M}'$. 如是在 n 維模與非奇異的 n 級方陣間建立了對應關係. 今問對應於同一模之不同的底的方陣間之關係如何?

設 $z_1, \cdots, z_n$ 是 $\mathfrak{M}$ 的另一底,其對應之方陣爲 $B = (b_{ij})$,

$$\begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} \cdots b_{1n} \\ b_{21} & b_{22} \cdots b_{2n} \\ \cdots & \cdots \\ b_{n1} & b_{n2} \cdots b_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

由於 $y_1, \cdots, y_n$ 及 $z_1, \cdots, z_n$ 都是底,故有二方陣 $U = (u_{ij})$, $V = (v_{ij})$ 使

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = U \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}, \quad \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = V \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

於是由 $y_1, \cdots, y_n$ 之線性無關性及

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = UV \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix},$$

可知 $UV = I$, 卽 U 及 V 是模方陣. 今

$$\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = V \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = VA \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},$$

故得

$$B = VA. \tag{3}$$

故對應於同一模之二方陣是左結合的．反之，二非奇異的左結合方陣對應於同一模．故若將所有的 n 級非奇異方陣依左結合關係分類，則每一類代表一模，且不同的類所代表的模也不同．以後凡說到“模 $\mathfrak{M}$ 對應於方陣 A”，此 A 卽表示模 $\mathfrak{M}$ 所對應的一類方陣中的一個．

於是由定理 4.1，可知 n 維模 $\mathfrak{M}$ 之底 $y_1, \cdots, y_n$ 可取成如下的形式：

$$\begin{aligned} y_1 &= a_{11} x_1, \\ y_2 &= a_{21} x_1 + a_{22} x_2, \\ &\cdots\cdots\cdots\cdots \\ y_n &= a_{n1} x_1 + a_{n2} x_2 + \cdots + a_{nn} x_n, \end{aligned} \tag{4}$$

其中 $a_{\nu\nu} > 0$ $(1 \leqslant \nu \leqslant n)$，且 $0 \leqslant a_{\mu\nu} < a_{\nu\nu}$ $(\mu > \nu)$．此乃底之標準形式，或稱之爲標準底．

定理 3. 模 $\mathfrak{M}$ 包有模 $\mathfrak{N}$ 的充要條件是模 $\mathfrak{M}$ 所對應的方陣右除盡模 $\mathfrak{N}$ 所對應的方陣．

證：命 $\mathfrak{M}$ 及 $\mathfrak{N}$ 之底分別爲 $y_1, \cdots, y_n$ 及 $z_1, \cdots, z_n$，所對應的方陣分別爲 $A = (a_{ij})$ 及 $B = (b_{ij})$．若 $\mathfrak{M}$ 包有 $\mathfrak{N}$，則有

$$\begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix} = (c_{ij}) \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = (c_{ij})\,(a_{ij}) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = (b_{ij}) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

故得 $B = CA$．

反之，若 $B = CA$，則有

$$\begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix} = C A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = C \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}.$$

故 $\mathfrak{M}$ 包有 $\mathfrak{N}$．

定義 3. 若二線性型 z_1 與 z_2 之差在模 $\mathfrak{M}$ 中，則稱 z_1 與 z_2 對 mod $\mathfrak{M}$ 同餘，以 $z_1 \equiv z_2 \pmod{\mathfrak{M}}$ 表之．

顯然此同餘關係亦有反身，對稱，傳遞等三種性質，故可將所有線性型依 mod $\mathfrak{M}$ 分類：屬於同一類者互相同餘，不同類者決不同餘．如是所分成之類的

數目名爲 $\mathfrak{M}$ 之矩,以 $N(\mathfrak{M})$ 記之 (其存在性還未證明). 顯然 $\mathfrak{M}$ 本身卽爲其中之一類.

定理 4. 若模 $\mathfrak{M}$ 對應於方陣 A, 則

$$N(\mathfrak{M}) = |A|.$$

證: 由於 $\mathfrak{M}$ 所對應之方陣的行列式的絕對值都相同, 故不妨假定底已取標準形式 (4). 任一線性型

$$y = a_1 x_1 + \cdots + a_{n-1} x_{n-1} + a_n x_n$$

可減以 $y_n = a_{n1} x_1 + \cdots + a_{nn} x_n$ 之整數倍, 使適合於 $0 \leqslant a_n < a_{nn}$; 又可減以 $y_{n-1} = a_{n-1,1} x_1 + \cdots + a_{n-1,n-1} x_{n-1}$ 之整數倍,使適合於 $0 \leqslant a_{n-1} < a_{n-1,n-1}$, 等等. 故任一線性型必與一形如

$$a_1 x_1 + \cdots + a_n x_n, \qquad 0 \leqslant a_\nu < a_{\nu\nu} \quad (1 \leqslant \nu \leqslant n)$$

之線性型同餘. 此種線性型之數目爲 $a_{11} a_{22} \cdots a_{nn} = |A|$, 又此 $|A|$ 個線性型中無二者同餘,故得定理.

由定理 3 及定理 4 卽得

定理 5. 若 $\mathfrak{M} \supseteq \mathfrak{N}$, $\mathfrak{M}, \mathfrak{N}$ 所對應之方陣分別爲 A, B, 則依 mod $\mathfrak{N}$ 將 $\mathfrak{M}$ 中之元素分類,所得之類數爲 $\dfrac{N(\mathfrak{N})}{N(\mathfrak{M})} = \dfrac{|B|}{|A|}$.

由未定量 $x_1, \cdots, x_n$ 表出的集合 $\mathfrak{O} = \{x_1, \cdots, x_n\}$ 也可由其他未定量表出. 如命

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} u_{11} \cdots u_{1n} \\ \cdots\cdots\cdots\cdots \\ u_{n1} \cdots u_{nn} \end{pmatrix} \begin{pmatrix} x_1' \\ \vdots \\ x_n' \end{pmatrix},$$

此處 $U = (u_{ij})$ 爲一模方陣, 則 $x_1', \cdots, x_n'$ 也表出 $\mathfrak{O}$, 卽 $\mathfrak{O} = \{x_1, \cdots, x_n\} = \{x_1', \cdots, x_n'\}$.

若模 $\mathfrak{M}$ 及其一底 $y_1, \cdots, y_n$ 對未定量 $x_1, \cdots, x_n$ 對應於方陣 A, 今問對未定量 $x_1', \cdots, x_n'$ 對應於何方陣. 由

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = A\,U \begin{pmatrix} x_1' \\ \vdots \\ x_n' \end{pmatrix},$$

即知對未定量 $x'_1, \cdots, x'_n$, 對應之方陣爲 AU, 即右結合關係表示未定量的變換, 亦即表示 $\mathfrak{O}$ 的換底. 又由 (3) 已知左結合關係表示模的換底, 故由定理 5.1 可知: 對固定的 n 維模 $\mathfrak{M}$, 可經過模的換底及 $\mathfrak{O}$ 的換底, 使其對應之方陣化爲對角線方陣

$$[d_1, d_1 d_2, \cdots, d_1 \cdots d_n] \quad (d_1 > 0, \cdots, d_n > 0).$$

由定理 7.2 與定理 5 立得:

定理 6. 從任一 n 維模 $\mathfrak{M}$, 可以做出一鍊

$$\mathfrak{M} = \mathfrak{M}_0 \subset \mathfrak{M}_1 \subset \cdots \subset \mathfrak{M}_l = \mathfrak{O}, \tag{5}$$

使

$$N(\mathfrak{M}_{i-1}) / N(\mathfrak{M}_i) \qquad (1 \leqslant i \leqslant l)$$

是素數.

兩模 $\mathfrak{M}_1$ 及 $\mathfrak{M}_2$ 的所有公共元素成一模,此模稱爲 $\mathfrak{M}_1$ 與 $\mathfrak{M}_2$ 的交, 以 $\mathfrak{M}_m$ 記之. 又 $\mathfrak{M}_1$ 及 $\mathfrak{M}_2$ 中所有元素的和、差所成的集合也是一模, 此模稱爲 $\mathfrak{M}_1$ 與 $\mathfrak{M}_2$ 的和,以 $\mathfrak{M}_d$ 記之. 則有

定理 7. 設模 $\mathfrak{M}_1, \mathfrak{M}_2, \mathfrak{M}_m, \mathfrak{M}_d$ 分別對應於方陣 M_1, M_2, M_m, M_d, 則 M_m 爲 M_1, M_2 之最小公倍, M_d 爲 M_1, M_2 之最大公約.

證: 由 $\mathfrak{M}_1 \supseteq \mathfrak{M}_m$, $\mathfrak{M}_2 \supseteq \mathfrak{M}_m$, 得

$$M_m = A_1 M_1, \quad M_m = A_2 M_2.$$

若 $M_3 = B_1 M_1 = B_2 M_2$ 爲 M_1, M_2 之任一公倍, $\mathfrak{M}_3$ 爲 M_3 所對應之模,則

$$\mathfrak{M}_3 \subseteq \mathfrak{M}_1, \quad \mathfrak{M}_3 \subseteq \mathfrak{M}_2,$$

因而

$$\mathfrak{M}_3 \subseteq \mathfrak{M}_m, \qquad M_3 = CM_m.$$

即 M_m 爲 M_1, M_2 之最小公倍. 同樣可證 M_d 爲 M_1, M_2 之最大公約.

第 十 五 章

p-adic 數

§1. 引言. 本章之目的在於介紹 Hensel 的 p-adic 數概念，這一概念在數論、代數幾何、代數函數等方面都有廣泛的應用，已成爲近世代數中之一重要概念. 在進入嚴格的定義之前，先簡單介紹形式上如何獲得 p-adic 數的方法. 吾人回憶第二章中同餘式

$$f(x) \equiv 0 \pmod{p^l} \tag{1}$$

之解法，此處 $f(x)$ 爲一整係數多項式，p 爲一素數. 解此同餘式時，吾人係先解同餘式

$$f(x) \equiv 0 \pmod{p}. \tag{2}$$

若 (2) 式有一解 a_0，$0 \leqslant a_0 < p$，且

$$f'(a_0) \not\equiv 0 \pmod{p},$$

則命 $x = a_0 + py$，並討論同餘式

$$f(a_0 + py) \equiv 0 \pmod{p^2}, \qquad 0 \leqslant y < p,$$

即

$$f(a_0)/p + f'(a_0)\, y \equiv 0 \pmod{p}, \qquad 0 \leqslant y < p.$$

由此式唯一地定出 y，命之爲 a_1，如是，

$$x = a_0 + a_1 p, \qquad 0 \leqslant a_0 < p, \quad 0 \leqslant a_1 < p$$

乃同餘式

$$f(x) \equiv 0 \pmod{p^2}$$

之一解.

一般言之，若

$$x = x_0 = a_0 + a_1 p + a_2 p^2 + \cdots + a_{l-2} p^{l-2}, \quad 0 \leqslant a_\nu < p$$

是同餘式

$$f(x) \equiv 0 \pmod{p^{l-1}}$$

之一解，且

$$f'(x_0) \not\equiv 0 \pmod{p},$$

則命 $x = x_0 + p^{l-1}y$，並研究同餘式

$$f(x_0 + p^{l-1}y) \equiv 0 \pmod{p^l}, \qquad 0 \leqslant y < p,$$

卽

$$f(x_0) / p^{l-1} + f'(x_0)\, y \equiv 0 \pmod{p}, \qquad 0 \leqslant y < p.$$

由此唯一定出之 y，命之爲 a_{l-1}，則

$$x = a_0 + a_1 p + \cdots + a_{l-1} p^{l-1}, \qquad 0 \leqslant a_\nu < p$$

乃 (1) 式之一解.

此種手續可以行之無窮，形式上吾人可得一 p 之冪級數

$$a_0 + a_1 p + \cdots + a_l p^l + \cdots, \qquad 0 \leqslant a_\nu < p. \tag{3}$$

此冪級數稱爲方程式

$$f(x) = 0$$

之一 p-adic 解.

吾人已知，在用逐步接近法以求方程式 $f(x) = 0$ 之實數解時，若所行之次數愈多，亦卽小數點後所取之位數愈多，則所得之解就愈精確；在此，利用逐次解同餘式

$$f(x) \equiv 0 \pmod{p},$$
$$f(x) \equiv 0 \pmod{p^2},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$f(x) \equiv 0 \pmod{p^l},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$

以求方程式 $f(x) = 0$ 之 p-adic 解時，亦有類似之情形，卽所行之次數愈多，亦卽取 l 愈大，則最後一同餘式之解

$$x = a_0 + a_1 p + \cdots + a_{l-1} p^{l-1}, \qquad 0 \leqslant a_\nu < p$$

愈接近於原方程式之 p-adic 解.

抽象言之，形如 (3) 的 p 之冪級數謂之一 p-adic 數. 所當注意者，如此所得出者並非 p-adic 數之全部. 一般言之，p-adic 數准許有有限多個 p 的負冪，卽 p-adic 數之一般形式爲

$$a_{-n} p^{-n} + \cdots + a_0 + a_1 p + \cdots + a_l p^l + \cdots, \qquad 0 \leqslant a_\nu < p. \tag{4}$$

這和每一實數可以表爲 10 進位的無窮小數

$$a_{-n}10^n+\cdots+a_0+a_1 10^{-1}+\cdots+a_l 10^{-l}+\cdots,\qquad 0\leqslant a_\nu<10$$

相類似.

兩 p-adic 數

$$a_{-n}p^{-n}+\cdots+a_0+a_1p+\cdots+a_lp^l+\cdots,\qquad 0\leqslant a_\nu<p,$$

$$b_{-m}p^{-m}+\cdots+b_0+b_1p+\cdots+b_lp^l+\cdots,\qquad 0\leqslant b_\nu<p$$

之和及差卽爲其對應項之係數相加或相減後所得之冪級數

$$a_{-n}p^{-n}+\cdots+a_{-m-1}p^{-m-1}+(a_{-m}\pm b_{-m})p^{-m}+\cdots+(a_0\pm b_0)+$$
$$+(a_1\pm b_1)p+\cdots+(a_l\pm b_l)p^l+\cdots,$$

此處假定 $n\geqslant m$. 但若相加後所得之係數有大於或等於 p 者,則應向後進一位,例如 $a_\nu+b_\nu\geqslant p$, 則命 $(a_\nu+b_\nu)p^\nu=(a_\nu+b_\nu-p)p^\nu+p^{\nu+1}$, 把 $p^{\nu+1}$ 加到後一項中去;同樣若相減後係數有小於 0 者,則應向後借一位,例如 $a_\nu-b_\nu<0$, 則令 $(a_\nu-b_\nu)p^\nu+(a_{\nu+1}-b_{\nu+1})p^{\nu+1}+\cdots$ 爲 $(a_\nu-b_\nu+p)p^\nu+(a_{\nu+1}-b_{\nu+1}-1)p^{\nu+1}+\cdots$. 總之,最後使得所有之係數皆爲小於 p 之非負整數.

兩 p-adic 數之積同於通常冪級數之乘積,而所得之結果中亦應將大於或等於 p 之係數向後進位,直至所有之係數皆爲小於 p 之非負整數爲止.

例 1. 方程

$$3x=2$$

之 5-adic 解是

$$4+1\cdot5+3\cdot5^2+1\cdot5^3+3\cdot5^4+\cdots,$$

式中除去第一項外,其他各項之係數輪流爲 1,3 二數.

如欲證明此點,讀者可依解同餘式之方法進行. 但由下法亦可知此冪級數確爲所予方程式的 5-adic 解:

$$3\cdot(4+1\cdot5+3\cdot5^2+1\cdot5^3+3\cdot5^4+\cdots)=$$
$$=12+3\cdot5+9\cdot5^2+3\cdot5^3+9\cdot5^4+\cdots=$$
$$=2+(2+3)\cdot5+9\cdot5^2+3\cdot5^3+9\cdot5^4+\cdots=$$
$$=2+10\cdot5^2+3\cdot5^3+9\cdot5^4+\cdots=$$
$$=2+5\cdot5^3+9\cdot5^4+\cdots=$$
$$=2+10\cdot5^4+\cdots=$$

$$= \cdots$$

$$\cdots$$

$$= 2.$$

例 2. 方程

$$x^2 = 7$$

之一 3-adic 解是

$$1 + 1 \cdot 3 + 1 \cdot 3^2 + 0 \cdot 3^3 + 2 \cdot 3^4 + \cdots.$$

設 a 爲一有理數,方程 $x = a$ 的 p-adic 解謂之 a 的 p-adic 表示法.

最簡單的方程式 $x = d$ (d 爲正整數) 之 p-adic 解可逕由下法得之: 以 p 除 d, 其商爲 q_0, 餘數爲 d_0, 卽

$$d = d_0 + q_0 p, \quad 0 \leqslant d_0 < p.$$

再以 p 除 q_0, 其商爲 q_1, 餘數爲 d_1, 卽

$$d = d_0 + d_1 p + q_1 p^2, \quad 0 \leqslant d_0, d_1 < p.$$

如此繼續進行最後可得 d 之唯一的 p-adic 表示法

$$d_0 + d_1 p + d_2 p^2 + \cdots + d_l p^l, \quad 0 \leqslant d_\nu < p.$$

此卽爲以 p 爲底之記數法,如果我們不限定 p 是素數,例如取 p 爲 10, 則此卽爲普通之記數法.

因之整數之 p-adic 表示法與以 p 爲基數計算整數時之表示法全同.

習題 1. 求出方程 $x^2 = 7$ 之另一 3-adic 解.

習題 2. 求出方程 $x^2 + x + 1 = 0$ 之 7-adic 解.

習題 3. 求出方程 $9x^2 = 7$ 之 3-adic 解.

(提示: 先作變換 $3x = y$, 然後求 $y^2 = 7$ 之 3-adic 解,設爲 y_0, 則 $x_0 = 3^{-1}y_0$ 卽爲原方程式之 3-adic 解.)

§2. 賦值 (valuation) 之定義.

上節所述乃形式上的敍述方法,並沒有討論到冪級數

$$a_{-\nu} p^{-\nu} + \cdots + a_0 + a_1 p + \cdots + a_l p^l + \cdots, \quad 0 \leqslant a_\nu < p$$

之收斂問題,但此冪級數在通常的意義下是決不收斂的. 現在我們將引進一新觀念,藉此新觀念之助,使以上之冪級數具有嚴格之定義,且創造出新的數系. 此新觀念卽所謂賦值,它是實數裏絕對值觀念的抽象化, 並與絕對值具有相仿的性

質，其定義如下：

定義. 命 $a, b, \cdots$ 表有理數. 對任一有理數有一定有理數值的函數 ϕ, 若具有以下諸性質，則稱爲一賦值：

1) $\phi(a) \geqslant 0$, 其中等號當而且只當 $a=0$ 時成立；

2) $\phi(ab) = \phi(a)\ \phi(b)$；

3) $\phi(a+b) \leqslant \phi(a) + \phi(b)$.

由以上之定義可立得下之諸簡單性質：

由 2) 取 $a=b=1$, 及 1)，可知

$$\phi(1) = 1.$$

在 2) 中取 $a=b=-1$, 及 1)，可知

$$\phi(-1) = 1.$$

再在 2) 中取 $b=-1$, 可知

$$\phi(-a) = \phi(a).$$

又由 3)，可知對任一正整數 n, 常有

$$\phi(n) \leqslant \phi(1) + \phi(n-1) \leqslant \phi(1) + \phi(1) + \phi(n-2) \leqslant \cdots \leqslant n\,\phi(1) = n.$$

又由 3)，可知

$$\phi(a+b) \geqslant \phi(a) - \phi(b) \quad \text{或} \quad \phi(a+b) \geqslant \phi(b) - \phi(a).$$

例 1. 定義 $\phi(a) = 1$, 若 $a \neq 0$; $\phi(0) = 0$. 此 ϕ 顯然是一賦值，吾人稱之爲恆等賦值，並以 ϕ_0 記之，此種賦值不在討論之列。

例 2. 通常所用之絕對值 $\phi(a) = |a|$ 顯然是一賦值.

例 3. 命 p 表一固定之素數，則任一不等于 0 的有理數 a 可唯一地表爲

$$a = \frac{r}{s} p^n, \qquad s > 0,$$

此處 r, s 爲整數，$(r,s) = 1$, $p \nmid rs$, n 是一整數可爲正、負或零. 今定義

$$\phi(a) = p^{-n}, \quad a \neq 0; \quad \phi(0) = 0.$$

可證此 ϕ 爲一賦值，吾人稱之爲 p-adic 賦值，並記作 $\phi(a) = |a|_p$.

證：性質 1) 顯然適合.

若

$$a = \frac{r_1}{s_1} p^m, \quad b = \frac{r_2}{s_2} p^n \qquad (s_1 > 0, \quad s_2 > 0),$$

此處 r_1, s_1, r_2, s_2 爲整數，$(r_1, s_1) = (r_2, s_2) = 1$，$p \nmid r_1 s_1 r_2 s_2$，則

$$ab = \frac{r_1 r_2}{s_1 s_2} p^{m+n},$$

卽得

$$|ab|_p = p^{-(m+n)} = |a|_p \cdot |b|_p,$$

此卽性質 2)． 又並不失去普遍性，吾人可以假定 $m \leqslant n$，如是則

$$a + b = \frac{r_1 s_2 + r_2 s_1 p^{n-m}}{s_1 s_2} p^m,$$

由於 $p \nmid s_1 s_2$，因之

$$|a + b|_p \leqslant p^{-m} = |a|_p,$$

於是由 1) 卽得

$$|a + b|_p \leqslant |a|_p + |b|_p,$$

此卽性質 3)．

在此例的證明過程中，我們附帶地證明了

$$|a + b|_p \leqslant \max(|a|_p, |b|_p).$$

我們還可以證明：若 $|a|_p \neq |b|_p$，則

$$|a + b|_p = \max(|a|_p, |b|_p).$$

令 a, b 表示如上，並不妨假定 $m < n$，此時從

$$a + b = \frac{r_1 s_2 + r_2 s_1 p^{n-m}}{s_1 s_2} p^m,$$

及 $p \nmid (r_1 s_2 + r_2 s_1 p^{n-m})$ (因爲 $p \nmid r_1 s_1 r_2 s_2$)，卽得

$$|a + b|_p = p^{-m} = |a|_p = \max(|a|_p, |b|_p).$$

§ 3. 賦值之分類．

定義 1. 兩賦值 ϕ 及 ϕ' 間若有下之關係：不等式

$$\phi(a) < \phi(b) \quad 與 \quad \phi'(a) < \phi'(b)$$

同時成立，卽由前者得出後者，由後者亦得出前者，則稱此兩賦值爲等價．

命 $s > 0$，ϕ 爲一賦值，則 ϕ^s 亦適合 1) 及 2)，但 3) 不一定適合． 但若 $0 < s \leqslant 1$，則 3) 亦適合*，命 $\phi^s = \phi'$ $(0 < s \leqslant 1)$，則 ϕ' 亦爲一賦值，

---

*利用：若 $x \geqslant 0$, $y \geqslant 0$, $0 < s \leqslant 1$，則

$$(x + y)^s \leqslant x^s + y^s.$$

此式之證明：不妨假定 $x \leqslant y$，由

$$(x + y)^s - y^s = s\int_0^x (t + y)^{s-1}\, dt \leqslant sxy^{s-1} \leqslant x^s \qquad (x \geqslant 0,\ y \geqslant 0,\ 0 < s \leqslant 1),$$

卽得所證．

且易知 ϕ' 與 ϕ 等價.

定理 1. 設 ϕ 是一非恆等賦值,則與 ϕ 等價之賦值 ϕ' 乃 $\phi'=\phi^s$ $(s>0)$.

證: 由於 $\phi\neq\phi_0$, 故必有一有理數 a_0 使

$$0<\phi(a_0)<1$$

(若 $\phi(a_0)>1$, 則由 2),$\phi(a_0^{-1})<1$). 對任一有理數 $a\neq 0$, 今往討論適合於

$$\phi(a_0^m)<\phi(a^n)$$

之所有正整數對 (m,n), 亦卽適合於

$$(\phi(a_0))^m<(\phi(a))^n,$$

或卽

$$\frac{m}{n}>\frac{\log\phi(a)}{\log\phi(a_0)} \tag{1}$$

之所有正整數對 (m,n).

故

$$\frac{\log\phi(a)}{\log\phi(a_0)}$$

可以看作適合於 (1) 之所有有理數所成之集合的下限. 若 ϕ' 與 ϕ 等價,則由 ϕ' 所作出之表示式 $\frac{\log\phi'(a)}{\log\phi'(a_0)}$ 仍爲此有理數集合之下限. 因之對任一有理數 $a\neq 0$, 有

$$\frac{\log\phi(a)}{\log\phi(a_0)}=\frac{\log\phi'(a)}{\log\phi'(a_0)}.$$

此卽表示有只與 ϕ 及 ϕ' 有關而與 a 無關之正常數 s 存在,使

$$\frac{\log\phi'(a)}{\log\phi(a)}=\frac{\log\phi'(a_0)}{\log\phi(a_0)}=s>0,$$

卽

$$\phi'(a)=\phi^s(a)\quad(s>0).$$

此式對所有的有理數 $a\neq 0$ 都對,定理得證.

定義 2. 若有一正整數 $n_0(>1)$ 使

$$\phi(n_0)>1,$$

則該賦值稱爲亞幾米得賦值. 不然,卽對所有的正整數 n, 常有

$$\phi(n)\leqslant 1,$$

則該賦值稱爲非亞幾米得賦值.

例如絕對值 $\phi(a) = |a|$ 卽爲一亞幾米得賦值,恆等賦值 ϕ_0 及 p-adic 賦值 $\phi(a) = |a|_p$ 卽爲非亞幾米得賦值.

§4. 亞幾米得賦值.

定理 1. 任一亞幾米得賦值必與絕對值等價.

證: 設 ϕ 爲一亞幾米得賦值. 命 n 及 n' 表二大于 1 的正整數,將 n' 表爲

$$n' = a_0 + a_1 n + a_2 n^2 + \cdots + a_\nu n^\nu, \quad 0 \leqslant a_i < n, \quad a_\nu \neq 0 .$$

則

$$\phi(n') \leqslant \phi(a_0) + \phi(a_1)\,\phi(n) + \phi(a_2)\,\phi(n^2) + \cdots + \phi(a_\nu)\,\phi(n^\nu) ,$$

由於 $\phi(a_i) \leqslant a_i < n \ (i = 0, 1, \cdots, \nu)$,故得

$$\phi(n') \leqslant n\,(1 + \phi(n) + \phi(n)^2 + \cdots + \phi(n)^\nu) \leqslant$$
$$\leqslant n(1+\nu)\max(1, \phi(n)^\nu) .$$

由 n' 之表示式,可知 $n^\nu \leqslant n'$, 故 $\nu \leqslant \dfrac{\log n'}{\log n}$,由是

$$\phi(n') \leqslant n\left(1 + \frac{\log n'}{\log n}\right)\max(1, \phi(n)^{\log n'/\log n}) .$$

用 n'^h 代 n', 則得

$$\phi(n')^h \leqslant n\left(1 + h\,\frac{\log n'}{\log n}\right)\max(1, \phi(n)^{h\log n'/\log n}),$$

卽

$$\phi(n') \leqslant \left(n\left(1 + h\,\frac{\log n'}{\log n}\right)\right)^{1/h}\max(1, \phi(n)^{\log n'/\log n}) .$$

命 $h \to \infty$, 則得

$$\phi(n') \leqslant \max(1, \phi(n)^{\log n'/\log n}) . \tag{1}$$

此式對任一對正整數 $n, n'(>1)$ 皆眞實 (此處用了 $\lim\limits_{h\to\infty}(\alpha h + \beta)^{1/h} = 1$, $\alpha > 0$).*

由亞幾米得賦值之特性,知有一正整數 $n_0 > 1$, 使 $\phi(n_0) > 1$. 故得

$$1 < \max(1, \phi(n)^{\log n_0/\log n}),$$

---

* $\lim\limits_{h\to\infty}(\alpha h + \beta)^{1/h} = \lim\limits_{h\to\infty} e^{1/h\log(\alpha h+\beta)} = 1 \qquad (\alpha > 0)$.

由於此不等式中乃一開口號 ($<$),故得

$$\phi(n)^{\log n_0/\log n} > 1.$$

即對任一正整數 $n > 1$, 常有

$$\phi(n) > 1.$$

而 (1) 式變爲

$$\phi(n') \leqslant \phi(n)^{\log n'/\log n},$$

即

$$\frac{\log \phi(n')}{\log n'} \leqslant \frac{\log \phi(n)}{\log n}.$$

由於 n 及 n' 的對稱性,可得

$$\frac{\log \phi(n')}{\log n'} = \frac{\log \phi(n)}{\log n},$$

即有一祗與 ϕ 有關而與 n 無關的正常數 s 存在,使

$$\frac{\log \phi(n)}{\log n} = s > 0,$$

亦即對所有的正整數 $n > 1$, 常有

$$\phi(n) = n^s, \quad s > 0.$$

由 $\phi(n) \leqslant n$, 可得 $s \leqslant 1$.

由於 $\phi(-n) = \phi(n)$,故對所有的整數 n ($|n| > 1$),常有

$$\phi(n) = |n|^s, \quad 0 < s \leqslant 1.$$

由 2),知對所有的有理數 a, 常有

$$\phi(a) = |a|^s, \quad 0 < s \leqslant 1.$$

此即定理.

§5. 非亞幾米得賦值.

在 §2 中研究 p-adic 賦值 $\phi(a) = |a|_p$ 時,吾人已證明下之不等式:

$$|a + b|_p \leqslant \max(|a|_p, |b|_p);$$

且若 $|a|_p \neq |b|_p$, 則

$$|a + b|_p = \max(|a|_p, |b|_p).$$

今往證明對一般的非亞幾米得賦值亦有此種性質.

定理 1. 設 ϕ 爲一非亞幾米得賦值,則有不等式

3′) $$\phi(a + b) \leqslant \max(\phi(a), \phi(b)).$$

且若 $\phi(a) \neq \phi(b)$,則有

$$3'') \qquad \phi(a+b) = \max(\phi(a), \phi(b)).$$

反之,若賦值 ϕ 適合不等式 3′),則 ϕ 爲非亞幾米得賦值。

證: 由二項式定理

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1} b + \cdots + \binom{n}{n-1} a b^{n-1} + b^n,$$

及由非亞幾米得賦值的特性,對任意的正整數 n 常有 $\phi(n) \leqslant 1$,因之

$$\phi((a+b)^n) \leqslant \phi(a)^n + \phi(a)^{n-1}\phi(b) + \cdots + \phi(a)\phi(b)^{n-1} + \phi(b)^n \leqslant$$
$$\leqslant (n+1)\max(\phi(a)^n, \phi(b)^n),$$

卽

$$\phi(a+b) \leqslant (n+1)^{1/n}.\max(\phi(a), \phi(b)).$$

命 $n \to \infty$,卽得 3′).

若 $\phi(a) \neq \phi(b)$,不妨假定 $\phi(b) < \phi(a)$. 由 3′) 已知

$$\phi(a+b) \leqslant \phi(a).$$

若 $\phi(a+b) < \phi(a)$,則由 3′) 可得

$$\phi(a) = \phi((a+b)-b) \leqslant \max(\phi(a+b), \phi(b)) < \phi(a),$$

此乃一矛盾,故得

$$\phi(a+b) = \phi(a) = \max(\phi(a), \phi(b)).$$

反之,若一賦值 ϕ 適合 3′),則對任一正整數 n,有

$$\phi(n) = \phi(1+1+\cdots+1) \leqslant \phi(1) = 1,$$

卽 ϕ 爲一非亞幾米得賦值,定理得證.

由上之定理,可知要證明一函數 ϕ 爲非亞幾米得賦值只要證明其具有性質 1),2) 及 3′) 卽可. 同時可知對非亞幾米得賦值 ϕ, $\phi^s (s>0)$ 仍爲一賦值,而不必假定 $s \leqslant 1$. 蓋此時由 3′) 可得

$$\phi^s(a+b) \leqslant \max(\phi^s(a), \phi^s(b)) \leqslant \phi^s(a) + \phi^s(b),$$

此卽 3) 也.

對非亞幾米得賦值 ϕ,命

$$w(a) = -\log\phi(a).$$

此對數以任一大於 1 之實數爲底. 底之選擇並無太大關係,因爲 $\phi^s (s>0)$ 仍

爲一非亞幾米得賦值。

由 ϕ 之性質可得出 w 之次諸性質:

i) 若 $a \neq 0$, 則 $w(a)$ 爲實數, $w(0) = \infty$;

ii) $w(ab) = w(a) + w(b)$;

iii) $w(a+b) \geqslant \min(w(a), w(b))$;

iii′) $w(a+b) = \min(w(a), w(b))$, 若 $w(a) \neq w(b)$.

若 ϕ 非恆等賦值,則必有有理數 a_0, 使

$$0 < w(a_0) < \infty.$$

由 ϕ 之性質,還可知

$$w(-a) = w(a), \quad w(1) = 0,$$

及對所有之整數 n, 常有

$$w(n) \geqslant 0.$$

定理 2. 兩非恆等的非亞幾米得賦值 ϕ 與 ϕ' 等價的充分且必要條件是: 對任一有理數 a $(a \neq 0)$,有

$$w'(a) = sw(a) \quad (s > 0),$$

其中 $w'(a) = -\log \phi'(a)$, $w(a) = -\log \phi(a)$.

證: 顯然.

定理 3. 任一非恆等的非亞幾米得賦值 ϕ 必與 p-adic 賦值 $|a|_p$ 等價.

證: 對任一整數 n 常有 $w(n) \geqslant 0$. 因 $\phi \neq \phi_0$, 故必有整數 $m(\neq 1)$,使

$$w(m) > 0.$$

今往證所有適合上式之整數所成之集合成一模: 若 $w(n) > 0$, $w(n') > 0$, 則由 iii) 卽得

$$w(n \pm n') \geqslant \min(w(n), w(n')) > 0.$$

由是由定理 1.4.3 知此模中有一最小的正整數 g 存在,凡該模中之任一數必爲 g 之倍數.

今往證 g 是一素數. 顯然 $g > 1$. 其次

$$g \neq g'g'', \quad g' > 1, \quad g'' > 1.$$

不然,則

$$w(g) = w(g'g'') = w(g') + w(g''),$$

由於 $w(g) > 0$ 及 $w(g') \geqslant 0$, $w(g'') \geqslant 0$, 故必有 $w(g') > 0$ 或 $w(g'') > 0$, 但 $1 < g' < g$, $1 < g'' < g$, 此與 g 之定義矛盾, 故 g 是一素數,命 $g = p$. 由是,已證明了

$$w(n) = 0, \quad p \nmid n,$$
$$w(n) > 0, \quad p \mid n.$$

對任一不爲 0 的有理數 a, 吾人可唯一地表成爲

$$a = \frac{r}{s} p^l, \qquad s > 0.$$

此處 r,s 爲整數, $(r,s) = 1$, 且 $p \nmid rs$, l 爲整數. 由是得

$$\begin{aligned} w(a) &= w\left(\frac{r}{s}\right) + lw(p) = \\ &= w(r) - w(s) + lw(p) = \\ &= lw(p). \end{aligned}$$

今

$$w'(a) = -\log|a|_p = l \log p,$$

故得

$$w(a) = \frac{w(p)}{\log p} w'(a).$$

命 $\dfrac{w(p)}{\log p} = s$, 由定理 2 卽得本定理.

§ 6. 有理數之 ϕ-擴張.

讀者如已有高等分析之知識,在學習本節及以後各節時,可與 Cantor 的實數構成理論參酌比較,較易領會.

命 ϕ 是一賦值. 今用 $\{a_n\}$ 代表有理數貫,卽

$$a_1, a_2, \cdots, a_n, \cdots, \tag{1}$$

其中每一項皆爲有理數.

定義 1. 數貫 $\{a_n\}$ 之適合以下之條件者謂之基貫,或 ϕ-收斂貫: 對任一有理數 $\varepsilon > 0$, 有一正整數 $N(=N(\varepsilon))$ 存在,使當 $m, n > N$ 時,

$$\phi(a_m - a_n) < \varepsilon.$$

例如: $a_1 = a_2 = \cdots = a_n = \cdots = a$ (a 有理數) 卽爲一基貫, 此基貫以 $\{a\}$ 表之.

若 $\{a_n\}$ 是一基貫,則 $\phi(a_n) \leqslant A$, A 是一與 n 無關的正整數.

兩貫 $\{a_n\}$ 與 $\{b_n\}$ 之和、差及積定義如下:

$$\{a_n\} \pm \{b_n\} = \{a_n \pm b_n\}, \qquad \{a_n\} \cdot \{b_n\} = \{a_n b_n\}.$$

由

$$\phi((a_m \pm b_m) - (a_n \pm b_n)) \leqslant \phi(a_m - a_n) + \phi(b_m - b_n)$$

及

$$\phi(a_m b_m - a_n b_n) = \phi(a_m(b_m - b_n) + b_n(a_m - a_n)) \leqslant \phi(a_m)\,\phi(b_m - b_n) + \\ + \phi(b_n)\,\phi(a_m - a_n),$$

易知兩基貫之和、差及積仍為基貫.

定義 2. 對一數貫 $\{a_n\}$,如有一有理數 a 適合下之條件:對任一有理數 $\varepsilon > 0$,有正整數 $N(=N(\varepsilon))$ 存在,使當 $n > N$ 時,

$$\phi(a_n - a) < \varepsilon,$$

則稱數貫 $\{a_n\}$ 具有 ϕ-極限 a. 並記之為

$$\phi\text{-}\lim_{n\to\infty} a_n = a.$$

顯然,$\{a\}$ 的 ϕ-極限是 a. 利用 $\phi(a_m - a_n) \leqslant \phi(a_m - a) + \phi(a_n - a)$,可知有 ϕ-極限之貫是基貫. 但當注意者,並不是每一基貫皆有 ϕ-極限.

如 $\{a_n\}$ 及 $\{b_n\}$ 之 ϕ-極限分別是 a 及 b,則此二貫之和、差及積也有 ϕ-極限,而且分別是 $a+b$, $a-b$ 及 ab.

又若

$$\phi\text{-}\lim_{n\to\infty} a_n = a,$$

則

$$\lim_{n\to\infty} \phi(a_n) = \phi(a).$$

定義 3. 凡以 0 為 ϕ-極限之貫稱為零貫. 所有零貫所成之集合以 $\widetilde{0}$ 表示之.

例 1. 如 $\phi(a) = |a|$, 則 $\left\{a_n = \frac{1}{n}\right\}$ 是一零貫.

例 2. 如 $\phi(a) = |a|_p$, 則 $\{a_n = p^n\}$ 是一零貫.

極易證明:二零貫之和仍為一零貫,一零貫與一基貫之積是一零貫.

上面已經定義了兩貫之和、差及積. 今再定義兩貫的商:如 $\{b_n\}$ 非零貫,則 $\{b_n\}$ 除 $\{a_n\}$ 之商定義為

$$\{a_n b_n^{-1}\}.$$

注意: $\{b_n\}$ 雖非零貫,但 $\{b_n\}$ 中可能有為 0 之項,此時我們棄去這些等於 0 的 b_n, 對問題的討論並無影響.

如 $\{a_n\}$ 是一基貫,但非零貫,則必有一正有理數 c 及一正整數 N 存在,使當 $n > N$ 時,有

$$\phi(a_n) > c > 0.$$

今往證明: 兩基貫 $\{a_n\}, \{b_n\}$ ($\{b_n\}$ 非零貫) 之商 $\{a_n b_n^{-1}\}$ 仍為一基貫.

因為

$$\phi\{a_m b_m^{-1} - a_n b_n^{-1}\} = \phi\{(a_m(b_n - b_m) + b_m(a_m - a_n)) b_m^{-1} b_n^{-1}\} \leqslant$$

$$\leqslant \{\phi(a_m) \phi(b_n - b_m) + \phi(b_m) \phi(a_m - a_n)\} \phi^{-1}(b_m) \phi^{-1}(b_n).$$

對任一有理數 $\varepsilon > 0$, 有正整數 N_1 存在,使當 $n, m > N_1$ 時,

$$\phi(b_n - b_m) < \varepsilon, \quad \phi(a_m - a_n) < \varepsilon.$$

又知有一正有理數 c 及一正整數 A 存在,使當 $n,m > N_2$ 時

$$\phi(b_m) > c, \quad \phi(b_n) > c, \quad \phi(a_m) < A, \quad \phi(b_m) < A.$$

故得

$$\phi(a_m b_m^{-1} - a_n b_n^{-1}) \leqslant 2A\, c^{-2}\, \varepsilon, \quad n, m > N, \quad N = \max(N_1, N_2).$$

此即表明 $\{a_n b_n^{-1}\}$ 是一基貫.

定義 4. 若二基貫 $\{a_n\}, \{b_n\}$ 之差 $\{a_n - b_n\}$ 是一零貫,則稱此兩貫為同餘,並以

$$\{a_n\} \equiv \{b_n\} \pmod{\overline{\{0\}}}$$

表之.

此同餘關係顯然有下之三性質:

(i) $\{a_n\} \equiv \{a_n\} \pmod{\overline{\{0\}}}$;

(ii) 若 $\{a_n\} \equiv \{b_n\} \pmod{\overline{\{0\}}}$, 則 $\{b_n\} \equiv \{a_n\} \pmod{\overline{\{0\}}}$;

(iii) 若 $\{a_n\} \equiv \{b_n\} \pmod{\overline{\{0\}}}$, $\{b_n\} \equiv \{c_n\} \pmod{\overline{\{0\}}}$, 則

$\{a_n\} \equiv \{c_n\} \pmod{\overline{\{0\}}}$.

故利用同餘關係,可將所有的基貫分類: 屬於同一類之基貫皆同餘,不同類之兩

基貫決不同餘. 於每一類中任擇一基貫 $\{a_n\}$ 爲代表而以 $\overline{\{a_n\}}$ 表該類.

今往定義類之間的加、減、乘、除: 於兩類 $\overline{\{a_n\}}$ 及 $\overline{\{b_n\}}$ 中各取代表 $\{a_n\}$ 及 $\{b_n\}$, 定義

$$\overline{\{a_n\}} \pm \overline{\{b_n\}} = \overline{\{a_n \pm b_n\}},$$

$$\overline{\{a_n\}} \cdot \overline{\{b_n\}} = \overline{\{a_n b_n\}},$$

當 $\overline{\{b_n\}}$ 不是 $\overline{\{0\}}$ 時,定義

$$\overline{\{a_n\}} \cdot \overline{\{b_n\}}^{-1} = \overline{\{a_n b_n^{-1}\}}.$$

如上所定義的類之間的加、減、乘、除 $\overline{\{a_n \pm b_n\}}$, $\overline{\{a_n b_n\}}$, $\overline{\{a_n b_n^{-1}\}}$ 僅與類 $\overline{\{a_n\}}$ 及 $\overline{\{b_n\}}$ 有關而與代表之選擇無關,蓋由

$$\{a_n\} \equiv \{a_n'\} \pmod{\overline{\{0\}}} \quad 及 \quad \{b_n\} \equiv \{b_n'\} \pmod{\overline{\{0\}}}$$

可得出

$$\{a_n \pm b_n\} \equiv \{a_n' \pm b_n'\},\ \{a_n b_n\} \equiv \{a_n' b_n'\},\ 及\ \{a_n b_n^{-1}\} \equiv \{a_n' b_n'^{-1}\} \pmod{\overline{\{0\}}}$$

故也.

所有類所成之系統稱爲有理數之 ϕ-擴張, 每一類稱爲此 ϕ-擴張中之一數. 如果 $\phi(a) = |a|$, 則此 ϕ-擴張卽爲實數系統. 而當 $\phi(a) = |a|_p$ 時,此 ϕ-擴張名爲 p-adic 數系統. 至此, p-adic 數已有一嚴格之定義,以後還將進一步求出 p-adic 數的具體表示法.

所有類中包含類 $\overline{\{a\}}$ (a 有理數),此類中之任一基貫皆 ϕ-收斂於同一有理數 a, 卽以 a 爲 ϕ-極限,吾人遂以 $\overline{\{a\}} = a$ 記之. 所有如此之類與有理數全體成一一對應,由於基貫不一定 ϕ-收斂于有理數,故可知有理數之 ϕ-擴張爲較有理數系統更大的系統.

一般,吾人定義 $\overline{\{a_n\}}$ 卽爲此類中每一基貫所 ϕ-收斂的數,卽定義

$$\phi\text{-}\lim_{n\to\infty} a_n = \overline{\{a_n\}}.$$

此處應加以說明者,卽當 $\{a_n\}$,$\{a_n'\}$ 屬於同一類時, $\phi\text{-}\lim\limits_{n\to\infty} a_n = \phi\text{-}\lim\limits_{n\to\infty} a_n'$.

以上所討論之賦值只在有理數域上定義,現在我們把它的定義域擴大到有理數的 ϕ-擴張.

定 義 5. $$\phi(\overline{\{a_n\}})=\lim_{n\to\infty}\phi(a_n).$$

在此定義中必須說明一點,即 $\phi(\overline{\{a_n\}})$ 的定義與 $\{a_n\}$ 的選擇無關. 即若

$$\{a_n\}\equiv\{a_n'\}\pmod{\overline{\{0\}}},$$

則

$$\lim_{n\to\infty}\phi(a_n)=\lim_{n\to\infty}\phi(a_n').$$

此式之證明極易 (利用 $\phi(a_n)-\phi(a_n')\leqslant\phi(a_n-a_n')$).

爲簡便計,以後用希臘字母 $\alpha,\beta,\gamma,\cdots$ 表諸類. 易證 $\phi(\alpha)$ 亦具有下之三性質:

1) $\phi(\alpha)\geqslant 0$, $\phi(\alpha)=0$ 當且僅當 α 爲 $\overline{\{0\}}$;

2) $\phi(\alpha\beta)=\phi(\alpha)\phi(\beta)$;

3) $\phi(\alpha+\beta)\leqslant\phi(\alpha)+\phi(\beta)$.

習題 1. 證明由等價之兩賦值所得出的有理數擴張是相同的.

習題 2. 證明在非亞幾米得賦值之情況下: $\{a_n\}$ 收斂之必要且充分條件爲 $\lim\limits_{n\to\infty}\phi(a_{n+1}-a_n)=0$.

§ 7. 擴張之完整性.

在上節中我們從有理數的基貫出發,得到比有理數系統更大的有理數之 ϕ-擴張,同時我們已將 ϕ 之定義域從有理數系統擴充到有理數之 ϕ-擴張,即已經定義了 $\phi(\alpha)$. 今之問題在於: 如果在有理數之 ϕ-擴張上再運用上節之方法實行 ϕ-擴張 (此兩 ϕ 一致),是否能得出較有理數之 ϕ-擴張更大的系統. 如屬不能,則此系統謂之完整系統. 爲討論此問題,仿照前節,先定義以類爲項的基貫,ϕ-極限,零貫等等. 用 $\{\alpha_l\}$ 表由類所成之貫,即

$$\alpha_1,\ \alpha_2,\cdots,\alpha_l,\cdots,\tag{1'}$$

其中每一項皆爲一類.

定 義 1'. 貫 $\{\alpha_l\}$ 之適合于以下之條件者謂之基貫,或 ϕ-收斂貫: 對任一實數 $\varepsilon>0$, 必有一正整數 $L(=L(\varepsilon))$ 存在,使當 $l,k>L$ 時,

$$\phi(\alpha_l-\alpha_k)<\varepsilon.$$

定 義 2'. 對貫 $\{\alpha_l\}$, 如有一類 α 適合下之條件: 對任一實數 $\varepsilon>0$, 有正整數 $L(=L(\varepsilon))$ 存在,使當 $l>L$ 時,

$$\phi(\alpha_l-\alpha)<\varepsilon,$$

則稱貫 $\{\alpha_l\}$ 具有 ϕ-極限 α，並記之爲

$$\phi\text{-}\lim_{l\to\infty}\alpha_l=\alpha.$$

由此易知，若

$$\phi\text{-}\lim_{l\to\infty}\alpha_l=\alpha,$$

則

$$\lim_{l\to\infty}\phi(\alpha_l)=\phi(\alpha).$$

把每一有理數貫 $\{a_n\}$ 中之有理數 a_ν 視爲 $a_\nu=\overline{\{a_\nu\}}$，則在此新定義之下，每一有理數的 ϕ-收斂貫皆有有理數之 ϕ-擴張中的一數爲其 ϕ-極限.

定義 3′. 凡以 $\overline{\{0\}}=0$ 爲極限之貫稱爲零貫，所有零貫所成之集合以 $\widetilde{\{0\}}$ 表之.

兩貫之加、減、乘、除的定義也可仿上節說出.

定義 4′. 若兩基貫 $\{\alpha_l\}$ 及 $\{\beta_l\}$ 之差 $\{\alpha_l-\beta_l\}$ 爲一零貫，則稱此兩貫同餘. 並以

$$\{\alpha_l\}\equiv\{\beta_l\}\pmod{\widetilde{\{0\}}}$$

表之.

利用同餘關係，又可將所有基貫分類：屬於同一類之基貫皆同餘，不同類之基貫決不同餘. 於每一類中任擇一基貫 $\{\alpha_l\}$ 爲代表而以 $\widetilde{\{\alpha_l\}}$ 表該類.

和上節一樣，可以定義類之間的加、減、乘、除.

所有類所成之系統，稱之爲有理數之 ϕ-擴張之 ϕ-擴張（此兩 ϕ 一致）. 所有的類中包含類 $\widetilde{\{\alpha\}}$，此類中之任一基貫皆以 α 爲 ϕ-極限，吾人逕以 $\widetilde{\{\alpha\}}=\alpha$ 記之. 所有這種類與有理數之 ϕ-擴張成一一對應. 今之問題卽問此新擴張是否得出更大之系統？答案是否定的，此卽下之定理.

定理 1. 由有理數經賦值 ϕ-擴張而得出的系統是完整的，卽任一 ϕ-收斂貫 $\{\alpha_l\}$ 都有 ϕ-極限.

證：假定 $\{\alpha_l\}$ 是一 ϕ-收斂貫. 命 α_l 是 ϕ-收斂貫 $\{a_n^{(l)}\}$ 的 ϕ-極限，卽

$$\alpha_l=\phi\text{-}\lim_{n\to\infty}a_n^{(l)}.$$

故存在 $n_0 = n_0(l)$，使當 $n \geqslant n_0(l)$ 時，

$$\phi(\alpha_l - a_n^{(l)}) < \frac{1}{l}.$$

今往證明有理數貫

$$\left\{ a_{n_0(l)}^{(l)} \right\} \tag{1}$$

是 ϕ-收斂貫，且其 ϕ-極限卽為 $\{\alpha_l\}$ 之 ϕ-極限。

由

$$\phi(a_{n_0(l)}^{(l)} - a_{n_0(l')}^{(l')}) \leqslant \phi(a_{n_0(l)}^{(l)} - \alpha_l) + \phi(\alpha_l - \alpha_{l'}) + \phi(a_{n_0(l')}^{(l')} - \alpha_{l'}) \leqslant$$

$$\leqslant \frac{1}{l} + \phi(\alpha_l - \alpha_{l'}) + \frac{1}{l'}$$

及 $\{\alpha_l\}$ 是 ϕ-收斂貫，可知 (1) 是 ϕ-收斂貫。命

$$\phi\text{-}\lim_{l\to\infty} a_{n_0(l)}^{(l)} = \alpha,$$

由

$$\phi(\alpha - \alpha_l) \leqslant \phi(\alpha - a_{n_0(l)}^{(l)}) + \phi(\alpha_l - a_{n_0(l)}^{(l)}),$$

可知

$$\phi\text{-}\lim_{l\to\infty} \alpha_l = \alpha.$$

§8. p-adic 數之表示法.

在本節中命 $\phi(a) = |a|_p$，研究 p-adic 數的表示法。

1) 先研究有理數

$$\frac{a}{b}, \quad (a, b) = 1, \quad p \nmid b$$

之 p-adic 表示法。為此，研究同餘式

$$bx \equiv a \pmod{p^l}, \quad 0 \leqslant x < p^l$$

之解。命其解為 x_l，吾人知

$$\left| \frac{a}{b} - x_l \right|_p \leqslant p^{-l}.$$

由是

$$\phi\text{-}\lim_{l\to\infty}\left(\frac{a}{b}-x_l\right)=0.$$

故

$$\frac{a}{b}=\phi\text{-}\lim_{l\to\infty}x_l.$$

在 §1 中吾人已定義出

$$x_l=a_0+a_1p+\cdots+a_{l-1}p^{l-1},\qquad 0\leqslant a_\nu<p.$$

由於

$$\phi(x_l-x_{l'})=\phi(a_lp^l+\cdots+a_{l'-1}p^{l'-1})\leqslant p^{-l}\phi(a_l)+\cdots+p^{-(l'-1)}\phi(a_{l'-1})\leqslant$$

$$\leqslant p^{-l}+\cdots+p^{-(l'-1)}=\frac{\frac{1}{p^l}-\frac{1}{p^{l'}}}{1-\frac{1}{p}}<\varepsilon\quad(l'>l>L(\varepsilon)).$$

所以 $\{x_l\}$ 是 ϕ-收斂的. 即以其在 ϕ-擴張中之極限

$$a_0+a_1p+\cdots+a_{l-1}p^{l-1}+\cdots,\quad 0\leqslant a_\nu<p$$

爲有理數 $\frac{a}{b}$ $(p\nmid b)$ 之 p-adic 表示法.

2) 其次,可得有理數

$$\frac{a}{b},\quad (a,b)=1,\quad p^m\,\|\,b\ (m\ 爲\ \geqslant 0\ 之整數)$$

的 p-adic 表示法爲

$$p^{-m}(a_0+a_1p+\cdots+a_lp^l+\cdots),\quad 0\leqslant a_\nu<p,\quad m\geqslant 0. \tag{1}$$

冪級數 (1) 卽爲有理數表爲 p-adic 數之一般形式.

如果在冪級數 (1) 中,有

$$a_{l+\nu}=a_{l+\nu+t}=a_{l+\nu+2t}=\cdots=a_{l+\nu+nt}=\cdots\quad(\nu=1,2,\cdots,t),$$

此處 l 和 t 爲固定的整數, $t\geqslant 1$, 則稱此冪級數是循環的. 此時可改寫如下:

$$p^{-m}((a_0+a_1p+\cdots+a_lp^l)+p^{l+1}(a_{l+1}+a_{l+2}p+\cdots+a_{l+t}p^{t-1})+$$
$$+p^{l+t+1}(a_{l+1}+a_{l+2}p+\cdots+a_{l+t}p^{t-1})+\cdots),$$

或簡書爲

$$p^{-m}(A+p^{l+1}B+p^{l+t+1}B+p^{l+2t+1}B+\cdots),$$

其中

$$A=a_0+a_1p+\cdots+a_lp^l,\quad B=a_{l+1}+a_{l+2}p+\cdots+a_{l+t}p^{t-1}.$$

定理 1. 有理數之 p-adic 表示法是 p 的循環的冪級數；反之 p 的循環的冪級數是有理數.

證: 1) 如果

$$\alpha = p^{-m}\{A + p^{l+1}B + p^{l+t+1}B + p^{l+2t+1}B + \cdots\},$$

此處

$$A = a_0 + a_1 p + \cdots + a_l p^l,\quad B = a_{l+1} + a_{l+2} p + \cdots + a_{l+t} p^{t-1},$$

則

$$\alpha p^m - A = p^{l+1}B + p^{l+t+1}B + p^{l+2t+1}B + \cdots =$$
$$= p^{l+1}B(1 + p^t + p^{2t} + \cdots).$$

因爲

$$1 + p^t + p^{2t} + \cdots + p^{kt} = \frac{1-p^{(k+1)t}}{1-p^t},$$

$$\left|\frac{1}{1-p^t} - \frac{1-p^{(k+1)t}}{1-p^t}\right|_p = p^{-(k+1)t} < \varepsilon \quad (k \geqslant k_0),$$

所以

$$1 + p^t + p^{2t} + \cdots + p^{kt} + \cdots = \frac{1}{1-p^t},$$

故得

$$\alpha p^m - A = p^{l+1}B \cdot \frac{1}{1-p^t},$$

卽

$$\alpha = p^{-m}A + p^{l+1-m}B \cdot \frac{1}{1-p^t},$$

故 α 爲一有理數.

2) 先討論有理數

$$\alpha = \frac{r}{s},\quad |\alpha| < 1,\quad (r, s) = 1,\quad s > 0,\quad r < 0,\quad p \nmid s. \tag{2}$$

設 p 的指數 (mod s) 爲 t, 卽 t 是適合下式的最小正整數

$$p^t \equiv 1 \pmod{s}.$$

命

$$1 - p^t = ms,\qquad m < 0,$$

則

$$\alpha = \frac{r}{s} = \frac{mr}{1-p^t}.$$

由於 $|\alpha|<1$，故 mr 可表爲

$$mr=b_0+b_1p+\cdots+b_{t-1}p^{t-1},\qquad 0\leqslant b_i<p.$$

於是

$$\alpha=(b_0+b_1p+\cdots+b_{t-1}p^{t-1})(1+p^t+p^{2t}+\cdots)=$$
$$=(b_0+b_1p+\cdots+b_{t-1}p^{t-1})+p^t(b_0+b_1p+\cdots+b_{t-1}p^{t-1})+\cdots.$$

此表明 α 可表爲 p 的循環的冪級數.

其次,對任意的正有理數 α，設 $\alpha=a/b$，$(a,b)=1$，$p^m\parallel b$，則 α 可表成

$$p^m\alpha=a_0+a_1p+\cdots+a_vp^v+\frac{r}{s},\qquad 0\leqslant a_i<p,$$

其中 $\frac{r}{s}$ 或爲 0 或合于 (2) 中各條件. 故亦可表爲 p 的循環的冪級數.

若 $-\alpha$ 爲一負有理數,則先求出 α 之表示法,再求

$$0=p+(p-1)p+(p-1)p^2+\cdots$$

與 α 之差,卽得 $-\alpha$ 之表示法,而且所得之 p 的冪級數也是循環的.

有理數的表示方法已得，今再述一般之情况. 先證如下之 p 的冪級數表 p-adic 數:

$$\alpha=p^{-m}(a_0+a_1p+a_2p^2+\cdots),\quad 0\leqslant a_v<p,\quad m\geqslant 0. \tag{3}$$

命

$$x_l=p^{-m}(a_0+a_1p+a_2p^2+\cdots+a_{l-1}p^{l-1}).$$

由於 $\{x_l\}$ 是 ϕ-收斂的,故其在有理數 ϕ-擴張中之極限

$$\alpha=p^{-m}(a_0+a_1p+a_2p^2+\cdots),\qquad 0\leqslant a_v<p,\quad m\geqslant 0$$

表一 p-adic 數.

已知形如 (3) 之 p 的冪級數表 p-adic 數，今問任一 p-adic 數如何表法? 由上節我們已經知道任一 p-adic 數卽爲一 ϕ-收斂貫 $\{a_l\}$ 在有理數之 ϕ-擴張中的極限,但任一有理數 a_l 可表爲

$$a_l=p^{-m_l}(a_0^{(l)}+a_1^{(l)}p+\cdots),\quad 0\leqslant a_v^{(l)}<p.$$

若能證明 $\{a_l\}$ 在有理數 ϕ-擴張中之極限也可以這樣表出,則問題解決.

對任一正整數 t，存在一正整數 $L(=L(t))$，使當 $l,l'>L$ 時,有

$$|a_l-a_{l'}|_p<\frac{1}{p^t}.$$

這表明當 $l > L$ 時，$a_l, a_{l+1}, a_{l+2}, \cdots$ 表成 p 之冪級數時前面 $t+k$ 項（k 非負的整數）必須相同，由於 t 可以任意大，令 $t \to \infty$，卽得所證．

總之，我們已證明了一切形如 (3) 的 p 的冪級數（有限或無限）之全體卽爲 p-adic 數之全體．

§ 9. **應用．**

關於 p-adic 數之觀念雖在本章中方才出現，但在已往本書中已屢次出現．如本章開始所述之結果卽其一例． 此例可推廣爲有名之 Hensel 引．

定理 1 (Hensel)． 若 $f(x)$ 是一有整係數之多項式，且

$$f(x) \equiv g_0(x)\, h_0(x) \pmod p,$$

此處 $g_0(x)$ 及 $h_0(x)$ 爲互素之二多項式，則在 p-adic 數範圍之內有二多項式 $g(x) \equiv g_0(x)$，$h(x) \equiv h_0(x) \pmod p$ 使

$$f(x) = g(x)\, h(x).$$

證： 命 $g_l(x)$，$h_l(x)$ 爲二多項式適合

$$g_l(x) \equiv g_0(x), \qquad h_l(x) \equiv h_0(x) \pmod{p^l}$$

及

$$f(x) \equiv g_l(x)\, h_l(x) \pmod{p^l}.$$

顯然 g_l 與 h_l 互素 (mod p)． 命

$$g_{l+1}(x) = g_l(x) + p^l\, \phi(x)$$

及

$$h_{l+1}(x) = h_l(x) + p^l\, \psi(x),$$

則有

$$g_{l+1}(x)\, h_{l+1}(x) \equiv g_l(x)\, h_l(x) + p^l(\phi(x)\, h_l(x) + \psi(x)\, g_l(x)) \pmod{p^{l+1}}.$$

命

$$\frac{f(x) - g_l(x)\, h_l(x)}{p^l} \equiv t(x) \pmod p,$$

由於 $h_l(x)$ 及 $g_l(x)$ 爲互素 (mod p)，故有二多項式 $\phi(x)$ 及 $\psi(x)$ 使

$$t(x) \equiv \phi(x)\, h_l(x) + \psi(x)\, g_l(x) \pmod p.$$

故得

$$f(x) - g_{l+1}(x)\, h_{l+1}(x) \equiv f(x) - g_l(x)\, h_l(x) - p^l(\phi(x)\, h_l(x) + \psi(x)\, g_l(x)) \equiv$$
$$\equiv p^l(t(x) - \phi(x)\, h_l(x) - \psi(x)\, g_l(x)) \equiv$$

$$\equiv 0 \pmod{p^{l+1}}.$$

由於 $t(x)$ 之次數不超過 $g_l(x)\ h_l(x)$ 之次數，故可假定 $\phi(x)$ 之次數 $\leqslant g_l(x)$ 之次數，及 $\psi(x)$ 之次數 $\leqslant h_l(x)$ 之次數. $g_l(x)$ 與 $h_l(x)$ 之係數皆爲 ϕ-收斂，收斂於 $g(x)$ 與 $h(x)$，故得定理.

附記：請參考引 7.10.1，可以 p-adic 數之觀念說明之.

第 十 六 章

代 數 數 論 介 紹

§1. 代數數.

定義 1. 若 ϑ 爲一係數爲有理數的代數方程

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0 \tag{1}$$

的根,則 ϑ 稱爲代數數.

例如全體有理數,以及 $\sqrt{2}$, $i = \sqrt{-1}$ 等等都是代數數.

若對 (1) 施行通分法,得有有理整係數* 的代數方程. 因此代數數也可定義爲"有有理整係數的代數方程的根".

若 (1) 式爲不可化,且 $a_n \neq 0$, 則稱 $n = \partial^0 f$ 爲 ϑ 的次數,易見有理數的次數爲 1; i 的次數爲 2.

若 (1) 式爲不可化,並以

$$\vartheta^{(1)}, \vartheta^{(2)}, \cdots, \vartheta^{(n)} \tag{2}$$

表示 $f(x) = 0$ 所有的根,則由定理 4.2.2 可知 $\vartheta^{(j)} \neq \vartheta^{(k)}$ $(j \neq k)$,且若某一 $\vartheta^{(j)}$ 適合一有理係數方程 $g(x) = 0$, 則其他 $n-1$ 個根亦必適合此方程. 由是可知一代數數的次數是唯一確定的.

定理 1. 二代數數之和、差、積、商 (除數非 0) 仍爲代數數.

證: 僅舉和爲例證之,其他之證法與之相類似,讀者自證之.

設代數數 α 及 β 各適合於

$$f(x) = 0, \qquad g(x) = 0,$$

$f(x), g(x)$ 均爲有有理係數的多項式,且 $\partial^0 f = m$, $\partial^0 g = n$. 命

$$\alpha = \alpha^{(1)}, \alpha^{(2)}, \cdots, \alpha^{(m)}; \qquad \beta = \beta^{(1)}, \beta^{(2)}, \cdots, \beta^{(n)}.$$

---

*在本章中,爲了與"代數整數"區別起見,特稱普通的整數爲有理整數.

表示 $f(x)=0$, $g(x)=0$ 的根的全體,則 $\alpha+\beta$ 爲

$$h(x)=\prod_{j=1}^{m}\prod_{k=1}^{n}(x-(\alpha^{(j)}+\beta^{(k)}))=0$$

的根,但 $h(x)$ 的係數爲 $\alpha^{(j)}$ 及 $\beta^{(k)}$ 的對稱多項式,故由對稱多項式的定理,可知 $h(x)$ 也爲有有理係數的多項式. 定理得證.

定義 2. 若 ϑ 爲一首項係數爲 1, 其他係數爲有理整係數的不可化代數方程的根,則 ϑ 稱爲代數整數.

易見全體有理整數,以及 $\sqrt{2}$, i, $\frac{1+\sqrt{5}}{2}$ 等都是代數整數. 又易證:

定理 2. 代數整數之爲有理數者必爲有理整數.

定理 3. 二代數整數之和、差、積還是代數整數.

證明一如定理 1.

定理 4. 若 ϑ 爲一代數數,則必有自然數 q, 使 $q\vartheta$ 爲代數整數.

證: 若 ϑ 適合於

$$a_n\vartheta^n+a_{n-1}\vartheta^{n-1}+\cdots+a_0=0,\quad a_n>0,$$

其中諸 a 都是有理整數. 則因

$$(a_n\vartheta)^n+a_{n-1}(a_n\vartheta)^{n-1}+\cdots+a_0a_n^{n-1}=0,$$

故 $a_n\vartheta$ 爲代數整數.

定義 3. 若 ϑ 及 ϑ^{-1} 都是代數整數,則 ϑ 稱爲單位數.

例如 i, $3-2\sqrt{2}$ 都是單位數.

定理 5. ϑ 爲單位數的充分必要條件爲 ϑ 必須適合一個首項係數爲 1, 而末項係數爲 ±1 的有理整係數方程.

證: 因若 ϑ 適合於

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0=0,$$

則 ϑ^{-1} 適合於

$$a_0x^n+\cdots+a_{n-1}x+a_n=0,$$

故得定理.

習題 1. 試證係數爲代數數的代數方程的根還是代數數.

習題 2. 試證首項係數爲 1, 且有代數整數爲係數的代數方程的根還是代數整數.

習題 3. 試證以代數整數爲係數，且首項末項係數皆爲單位數的方程之根還是單位數.

§ 2. **代數數域.**

定義 1. 設 F 爲一由複數所成的集合，若 F 中至少含有二個不同的數，並且對於 F 中的任意二數，他們的和、差、積、商（除數非 0）也在 F 中時，則稱 F 爲一數域，或簡稱爲域.

例 1. 全體有理數構成一域. 今後常以 R 記之.

顯然，任一域中必包有 $\frac{\vartheta}{\vartheta}=1$ 及 $\vartheta-\vartheta=0$，所以亦包有 $1+1=2$, $1+2=3, \cdots, 1+(n-1)=n$ 及 $0-n=-n$，即包有所有的有理整數，因此亦包含所有的有理數. 故任一數域必包有有理數域 R.

例 2. 全體實數成一域.

例 3. 全體複數成一域.

例 4. 由定理 1.1，全體代數數也構成一域.

例 5. 易證所有形如 $a+bi$ (a, b 爲有理數) 的複數也成一域.

定理 1. 命 ϑ 是一 n 次代數數，則所有形如

$$a_0+a_1\vartheta+a_2\vartheta^2+\cdots+a_{n-1}\vartheta^{n-1}\quad (a_k \text{ 爲有理數}) \tag{1}$$

之數成一域，且 (1) 式所表之數各不相同.

證：若

$$a_0+a_1\vartheta+a_2\vartheta^2+\cdots+a_{n-1}\vartheta^{n-1}=b_0+b_1\vartheta+b_2\vartheta^2+\cdots+b_{n-1}\vartheta^{n-1},$$

而 a_k 並不全等於 b_k，則 ϑ 適合於一個次數不高於 $n-1$ 的代數方程，這與 ϑ 爲 n 次代數數的假定相矛盾，故由 (1) 式所表示之數各不相同.

再證所有形如 (1) 式之數成一域. 命 $f(x)=0$ 爲 ϑ 所適合的不可化方程，又命

$$\alpha=a(\vartheta)=a_0+a_1\vartheta+\cdots+a_{n-1}\vartheta^{n-1},$$
$$\beta=b(\vartheta)=b_0+b_1\vartheta+\cdots+b_{n-1}\vartheta^{n-1}.$$

顯見 $\alpha\pm\beta$ 亦爲 (1) 之形式. 又由定理 4.1.1 知有 $q(x)$ 及 $r(x)$ 使

$$a(x)\,b(x)=q(x)\,f(x)+r(x),\qquad \partial^0 r<\partial^0 f=n,$$

$q(x)$ 及 $r(x)$ 均爲有理係數多項式. 以 $x=\vartheta$ 代入，得

$$\alpha\beta = a(\vartheta)\,b(\vartheta) = r(\vartheta)$$

仍爲 (1) 之形式. 最後若 β 不等於 0, 則 $b(x)$ 與 $f(x)$ 互素,故有有理係數多項式 $s(x)$ 及 $t(x)$, 其中 $s(x)$ 之次數低於 n, 使

$$s(x)\,b(x) + t(x)\,f(x) = 1.$$

以 $x = \vartheta$ 代入,得到 $\frac{1}{\beta} = s(\vartheta)$, 故可知 $\frac{\alpha}{\beta} = \frac{1}{\beta}\alpha$ 亦爲 (1) 之形式. 定理得證.

定義 2. 定理 1 中所得之域謂之在有理數域 R 上添加 ϑ 所得之單擴張, 以 $R(\vartheta)$ 表之.

例 5 所述之域卽爲 $R(i)$.

定理 2. 若 $\vartheta \neq 0$, 則 $R(\vartheta)$ 卽爲由代數數 ϑ 經加、減、乘、除 (除數非 0) 所演出之數之最大集合.

其證甚易,讀者自證之.

定義 3. 由有限個代數數 $\vartheta_1, \cdots, \vartheta_l$ 經加、減、乘、除 (除數非 0) 所演出之域,謂之 R 上之有限擴張,以 $R(\vartheta_1, \cdots, \vartheta_l)$ 表之.

定理 3. 任何有限擴張必爲單擴張,卽對於任何有限擴張 $R(\vartheta_1, \cdots, \vartheta_l)$,可以找到代數數 ϑ, 使

$$R(\vartheta_1, \cdots, \vartheta_l) = R(\vartheta).$$

證: 僅就 $l = 2$ 的情形證明之. 由歸納法,極易推得一般的情形.

命 ϑ_1 及 ϑ_2 所適合的不可化方程各爲

$$f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 = 0,$$
$$g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0,$$

其中諸 a 及諸 b 均爲有理數. 又命此二式之根各爲

$$\vartheta_1 = \vartheta_1^{(1)}, \vartheta_1^{(2)}, \cdots, \vartheta_1^{(m)}; \qquad \vartheta_2 = \vartheta_2^{(1)}, \vartheta_2^{(2)}, \cdots, \vartheta_2^{(n)}.$$

取 h 爲一不同於所有的

$$\frac{\vartheta_2^{(u)} - \vartheta_2^{(v)}}{\vartheta_1^{(s)} - \vartheta_1^{(t)}} \qquad (1 \leqslant s, t \leqslant m, 1 \leqslant u, v \leqslant n)$$

的有理數,則 mn 個數 $h\vartheta_1^{(j)} + \vartheta_2^{(k)}$ $(1 \leqslant j \leqslant m,\ 1 \leqslant k \leqslant n)$ 各不相同.

命

$$\vartheta = h\,\vartheta_1 + \vartheta_2,$$

今將證明 $R(\vartheta) = R(\vartheta_1, \vartheta_2)$,祇須證明 ϑ_1, ϑ_2 均在 $R(\vartheta)$ 中,便已足够.

命

$$F(x) = \prod_{j=1}^{m} \prod_{k=1}^{n} (x - (h\vartheta_1^{(j)} + \vartheta_2^{(k)})),$$

$$H(x) = F(x) \sum_{j=1}^{m} \sum_{k=1}^{n} \frac{\vartheta_1^{(j)}}{x-(h\vartheta_1^{(j)}+\vartheta_2^{(k)})}.$$

由對稱多項式的定理,可知 $F(x)$ 及 $H(x)$ 均爲有有理係數的多項式. 以 $x = \vartheta$ 代入,因 $F(x) = 0$ 的根各不相同,故得

$$H(\vartheta) = F'(\vartheta)\,\vartheta_1, \qquad F'(\vartheta) \neq 0,$$

此處 $F'(\vartheta)$ 表示 $F(x)$ 在 $x = \vartheta$ 處的導數. 於是 $\vartheta_1 = \dfrac{H(\vartheta)}{F'(\vartheta)}$ 在 $R(\vartheta)$ 中,隨之 $\vartheta_2 = \vartheta - h\vartheta_1$ 也在 $R(\vartheta)$ 中,故得定理.

由此定理,今後祇須討論單擴張. 稱 $R(\vartheta)$ 爲代數數域, ϑ 的次數爲 $R(\vartheta)$ 的次數.

例 5 中之域 $R(i)$ 爲二次域. 有理數域 R 爲僅有的一次域.

定理 4. 若命 D 經過所有的不等於 1 的無平方因子的整數,則 $R(\sqrt{D})$ 經過所有的二次域.

證: 命 $R(\vartheta)$ 爲任一二次域,而命 ϑ 所適合的不可化方程爲

$$ax^2 + bx + c = 0,$$

其中 a, b, c 爲有理整數. 又命

$$b^2 - 4ac = q^2 D,$$

則因

$$\vartheta = \frac{-b \pm q\sqrt{D}}{2a}.$$

所以 $R(\vartheta) = R(\sqrt{D})$. 於是定理得證.

§3. 基底.

在本節中以 $R(\vartheta)$ 表示一 n 次代數數域. 記 $\vartheta = \vartheta^{(1)}$, 並命 $\vartheta^{(2)}, \cdots, \vartheta^{(n)}$ 表示 ϑ 所適合的不可化方程的其他 $n-1$ 個根.

由上節定理 1, $R(\vartheta)$ 中任一數 α 必可表成

$$\alpha = a(\vartheta) = a_0 + a_1 \vartheta + \cdots + a_{n-1} \vartheta^{n-1}$$

的形式，其中 a_i 爲有理數。

定義 1. 命 $\alpha^{(1)} = \alpha$，稱 $\alpha^{(k)} = a(\vartheta^{(k)})$ $(k = 2, 3, \cdots, n)$ 爲 α 的共軛數；又稱

$$S(\alpha) = \alpha^{(1)} + \cdots + \alpha^{(n)} = a(\vartheta^{(1)}) + \cdots + a(\vartheta^{(n)}),$$

$$N(\alpha) = \alpha^{(1)} \cdots \alpha^{(n)} = a(\vartheta^{(1)}) \cdots a(\vartheta^{(n)}),$$

爲 α 的跡與矩.

易見

$$S(\alpha + \beta) = S(\alpha) + S(\beta),$$

$$N(\alpha \beta) = N(\alpha) N(\beta).$$

由對稱多項式的定理，可知 $S(\alpha)$ 及 $N(\alpha)$ 均爲有理數，特別如 α 爲有理數，則 $S(\alpha) = n\alpha$, $N(\alpha) = \alpha^n$. 又若 α 爲代數整數，則 $\alpha^{(i)}$ 亦爲代數整數，故 $S(\alpha)$ 及 $N(\alpha)$ 均爲代數整數，但已知其爲有理數，故均爲有理整數.

若 α 爲單位數，則由 $N(\alpha)\ N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = N(1) = 1$ 及 $N(\alpha)$, $N(\alpha^{-1})$ 均爲有理整數可知 $N(\alpha) = \pm 1$. 反之，若 α 爲一代數整數，$N(\alpha) = \pm 1$. 則得 $\alpha^{-1} = \pm\, \alpha^{(2)} \cdots \alpha^{(n)}$ 亦爲代數整數，故 α 爲單位數. 故得：代數整數 α 爲單位數的充要條件是 $N(\alpha) = \pm 1$.

定理 1. 設 α 是 $R(\vartheta)$ 中之一數，命 α 所適合的不可化方程爲

$$h(x) = 0, \qquad \partial^0 h = l.$$

又命

$$g(x) = \prod_{\nu=1}^{n} (x - \alpha^{(\nu)}),$$

則 $g(x)$ 爲一有有理係數的多項式，且

$$g(x) = c(h(x))^{n/l},$$

其中 $l | n$, c 爲一有理數.

證： 由對稱多項式的定理，立刻得到 $g(x)$ 爲有有理係數的多項式.

命 $\alpha = a(\vartheta)$，則因

$$h(\alpha) = h(a(\vartheta)) = 0,$$

所以

$$h(\alpha^{(\nu)}) = h(a(\vartheta^{(\nu)})) = 0.$$

亦即 $g(x)=0$ 的每一個根,同時又爲 $h(x)=0$ 的根. 因 $h(x)$ 爲不可化多項式,今 $h(x)=0$ 與 $g(x)=0$ 有公根,故必 $h(x)|g(x)$. 命

$$g(x)=h(x)\,g_1(x).$$

若 $g_1(x)$ 爲一常數,則定理已得證;否則因 $g_1(x)=0$ 的根皆爲 $h(x)=0$的根,又有 $h(x)|g_1(x)$. 命

$$g_1(x)=h(x)\,g_2(x).$$

續行此法,因 $g(x)$ 之次數有限,故最後可得

$$g(x)=c(h(x))^{n/l},$$

定理得證.

由定理可知,若 α 是 l 次代數數,則在 $\alpha^{(1)},\cdots,\alpha^{(n)}$ 中,出現 l 個不同的數,且每數出現 n/l 次.

定義 2. 若在 $R(\vartheta)$ 中能找到一組數 $\alpha_1,\cdots,\alpha_m$, 使 $R(\vartheta)$ 中的任何一數,都可以唯一地表爲

$$a_1\alpha_1+\cdots+a_m\alpha_m$$

的形式,其中 $a_j\ (1\leqslant j\leqslant m)$ 爲有理數,則稱 $\alpha_1,\cdots,\alpha_m$ 爲 $R(\vartheta)$ 之基底.

易見 $\alpha_1,\cdots,\alpha_m$ 中之任一不能表爲其他 $m-1$ 個的係數爲有理數的線性組合.

由定理 2.1 可知 $1,\vartheta,\cdots,\vartheta^{n-1}$ 即爲 $R(\vartheta)$ 之一組基底,所以基底是存在的.

定理 2. $R(\vartheta)$ 之任一基底中所含元素之個數相同,且都等於 n.

證: 讀者可仿定理 14.9.2 補出.

若 $\alpha_1,\cdots,\alpha_n$ 及 $\beta_1,\cdots,\beta_n$ 爲 $R(\vartheta)$ 之兩組基底,則由定義,易知有有理數 $a_{jk}(1\leqslant j,\ k\leqslant n)$ 使

$$\alpha_j=\sum_{k=1}^{n}a_{jk}\beta_k \qquad (1\leqslant j\leqslant n),$$

且

$$|a_{jk}|=\begin{vmatrix}a_{11}\cdots a_{1n}\\ \cdots\cdots\cdots\cdots\\ a_{n1}\cdots a_{nn}\end{vmatrix}\neq 0.$$

定義 3. 設 $\alpha_1,\cdots,\alpha_n$ 是 $R(\vartheta)$ 中任意 n 個數. 稱

$$\Delta(\alpha_1,\cdots,\alpha_n)=\begin{vmatrix}\alpha_1^{(1)}\cdots\alpha_n^{(1)}\\ \cdots\cdots\cdots\cdots\\ \alpha_1^{(n)}\cdots\alpha_n^{(n)}\end{vmatrix}^2$$

爲 $\alpha_1,\cdots,\alpha_n$ 的判別式.

定理 3. 判別式有下列諸性質:

1) $\Delta(\alpha_1,\cdots,\alpha_n)$ 爲有理數,特別若 $\alpha_1,\cdots,\alpha_n$ 爲代數整數,則 $\Delta(\alpha_1,\cdots,\alpha_n)$ 爲有理整數.

2) 若 $\alpha_1,\cdots,\alpha_n$ 及 $\beta_1,\cdots,\beta_n$ 爲 $R(\vartheta)$ 的兩組基底, $\alpha_j=\sum_{k=1}^{n}a_{jk}\beta_k\ (1\leqslant j\leqslant n)$, 則

$$\Delta(\alpha_1,\cdots,\alpha_n)=|a_{jk}|^2\,\Delta(\beta_1,\cdots,\beta_n). \qquad (1)$$

換言之,對 $R(\vartheta)$ 之所有基底,其判別式之符號相同.

3) 若 $\alpha_1,\cdots,\alpha_n$ 爲 $R(\vartheta)$ 之一組基底, 則 $\Delta(\alpha_1,\cdots,\alpha_n)\neq 0$; 且反之亦眞.

證: 1) 由對稱多項式之定理立得所云.

2) 易知

$$\alpha_j^{(l)}=\sum_{k=1}^{n}a_{jk}\,\beta_k^{(l)}\qquad(1\leqslant j,l\leqslant n),$$

故

$$\Delta(\alpha_1,\cdots,\alpha_n)=\begin{vmatrix}\alpha_1^{(1)}\cdots\alpha_n^{(1)}\\ \cdots\cdots\cdots\cdots\\ \alpha_1^{(n)}\cdots\alpha_n^{(n)}\end{vmatrix}^2=\begin{vmatrix}a_{11}\cdots a_{1n}\\ \cdots\cdots\cdots\\ a_{n1}\cdots a_{nn}\end{vmatrix}^2\cdot\begin{vmatrix}\beta_1^{(1)}\cdots\beta_n^{(1)}\\ \cdots\cdots\cdots\cdots\\ \beta_1^{(n)}\cdots\beta_n^{(n)}\end{vmatrix}^2=$$

$$=|a_{jk}|^2\,\Delta(\beta_1,\cdots,\beta_n).$$

3) 因爲

$$\Delta(1,\vartheta,\cdots,\vartheta^{n-1})=\Big(\prod_{1\leqslant j<k\leqslant n}(\vartheta^{(j)}-\vartheta^{(k)})\Big)^2\neq 0,$$

故由 2) 可知對 $R(\vartheta)$ 之任何一組基底 $\alpha_1,\cdots,\alpha_n$ 有 $\Delta(\alpha_1,\cdots,\alpha_n)\neq 0$.

反之,若 $\Delta(\alpha_1,\cdots,\alpha_n)\neq 0$, 命

$$\alpha_j=\sum_{k=1}^{n}b_{jk}\,\vartheta^{k-1},$$

則

$$\Delta(\alpha_1,\cdots,\alpha_n)=|b_{jk}|^2\,\Delta(1,\vartheta,\cdots,\vartheta^{n-1}),$$

所以 $|b_{jk}|\neq 0$, 故能由 $\alpha_1,\cdots,\alpha_n$ 表出 $1,\vartheta,\cdots,\vartheta^{n-1}$, 即 $\alpha_1,\cdots,\alpha_n$ 成一基底.

定理 4. 假定 $\vartheta^{(1)},\cdots,\vartheta^{(n)}$ 中有 r_1 個實數, r_2 對共軛複數 $(r_1+2r_2=n)$, 則對 $R(\vartheta)$ 之任一基底 $\alpha_1,\cdots,\alpha_n$ 常有

$$(-1)^{r_2}\Delta(\alpha_1,\cdots,\alpha_n)>0.$$

證: 由定理 3, 今祗須考察 $\alpha_1=1,\ \alpha_2=\vartheta,\cdots,\alpha_n=\vartheta^{n-1}$ 之情况. 已知

$$\Delta(1,\vartheta,\cdots,\vartheta^{n-1})=\Big(\prod_{1\leqslant j<k\leqslant n}(\vartheta^{(j)}-\vartheta^{(k)})\Big)^2.$$

當 $\vartheta^{(k)}\neq\overline{\vartheta}^{(j)}$ 時 ($\overline{\vartheta}$ 表示 ϑ 之共軛複數),常有

$$((\vartheta^{(j)}-\vartheta^{(k)})(\overline{\vartheta}^{(j)}-\overline{\vartheta}^{(k)}))^2>0,$$

而

$$(\vartheta^{(j)}-\overline{\vartheta}^{(j)})^2<0,$$

故得

$$(-1)^{r_2}\Delta(1,\vartheta,\cdots,\vartheta^{n-1})>0.$$

§4. 整底.

在本章今後各節中,若無特別聲明,常以整數代表代數整數.

定義 1. 設 $\omega_1,\cdots,\omega_m$ 爲 $R(\vartheta)$ 中的 m 個整數,若 $R(\vartheta)$ 中之任一整數都能唯一地表爲如下的形式

$$a_1\omega_1+\cdots+a_m\omega_m,$$

其中 $a_1,\cdots,a_m$ 是有理整數,則稱 $\omega_1,\cdots,\omega_m$ 爲 $R(\vartheta)$ 之一組整底.

定理 1. 整底是存在的,更具體言之,基底

$$\omega_1,\cdots,\omega_n,$$

其中諸 $\omega_j(1\leqslant j\leqslant n)$ 皆爲整數,且使 $|\Delta(\omega_1,\cdots,\omega_n)|$ 之值爲最小者,爲一組整底.

證: 命 q 爲使 $q\vartheta$ 爲整數之自然數,則

$$1,\ q\vartheta,(q\vartheta)^2,\cdots,(q\vartheta)^{n-1}$$

全爲整數,且組成 $R(\vartheta)$ 之基底,故有 $\alpha_1,\cdots,\alpha_n$ 全爲整數的基底存在.

今證明使 $|\Delta(\alpha_1,\cdots,\alpha_n)|$ 之值最小之基底 $\omega_1,\cdots,\omega_n$ 即爲整底, 因若不然,則有整數

$$\omega=a_1\omega_1+\cdots+a_n\omega_n,$$

其中 a_i 不全爲有理整數．又不妨假定 a_1 不是有理整數．命 $a_1 = g + t$，g 爲一有理整數，而 $0 < t < 1$．則

$$\omega_1' = \omega - g\omega_1 = t\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n$$

也爲整數，且 $\omega_1', \omega_2, \cdots, \omega_n$ 也是 $R(\vartheta)$ 的基底．因

$$|\Delta(\omega_1', \omega_2, \cdots, \omega_n)| = t^2 |\Delta(\omega_1, \cdots, \omega_n)| < \\ < |\Delta(\omega_1, \cdots, \omega_n)|,$$

這與 $|\Delta(\omega_1, \cdots, \omega_n)|$ 取最小值之假定矛盾，故得證．

由此定理可知整底也是基底，故整底中所含元素的個數亦爲 n．

定理 2. 整底的判别式皆相等．即設 $\omega_1, \cdots, \omega_n$ 及 $\omega_1', \cdots, \omega_n'$ 爲 $R(\vartheta)$ 之兩組整底，則

$$\Delta(\omega_1, \cdots, \omega_n) = \Delta(\omega_1', \cdots, \omega_n').$$

證：因 $\omega_1, \cdots, \omega_n$ 及 $\omega_1', \cdots, \omega_n$ 均爲整底，故有

$$\omega_j = \sum_{k=1}^{n} a_{jk}\omega_k', \qquad \omega_j' = \sum_{k=1}^{n} b_{jk}\omega_k,$$

其中 a_{jk} 及 b_{jk} 皆爲有理整數．由此可得 $|a_{jk}|\cdot|b_{jk}| = 1$，即 $|a_{jk}| = \pm 1$，$|b_{jk}| = \pm 1$．故由定理 3.3 即得所證．

定義 2. 稱 $R(\vartheta)$ 的整底的判别式爲域之基數，以 Δ 或 $\Delta(R(\vartheta))$ 表之．

定理 3 (Stickelberger)．基數 $\Delta \equiv 0$ 或 $1 \pmod 4$．

證：以 $i_1, \cdots, i_n$ 表示 $1, 2, \cdots, n$ 的一種排列法，而 $\delta_{i_1,\cdots,i_n}$ 隨 $i_1, \cdots, i_n$ 爲偶排列或奇排列而爲 1 或 -1，於是由行列式之展開法，

$$\begin{vmatrix} \omega_1^{(1)} \cdots \omega_1^{(n)} \\ \cdots\cdots\cdots\cdots \\ \omega_n^{(1)} \cdots \omega_n^{(n)} \end{vmatrix} = \sum_{(i_1,\cdots,i_n)} \delta_{i_1,\cdots,i_n}\omega_1^{(i_1)}\cdots\omega_n^{(i_n)} =$$

$$= \sum_{(i_1,\cdots,i_n)} \omega_1^{(i_1)}\cdots\omega_n^{(i_n)} + 2\eta = a + 2\eta,$$

其中 η 爲一代數整數，而 $a = \sum_{(i_1,\cdots,i_n)} \omega_1^{(i_1)}\cdots\omega_n^{(i_n)}$ 爲 $\vartheta^{(1)}, \cdots, \vartheta^{(n)}$ 的對稱函數，故 a 爲有理數，因之亦爲有理整數．於是有

$$\Delta = (a + 2\eta)^2 = a^2 + 4\eta(\eta + a).$$

因整數 $\eta(\eta+a)=\frac{\Delta-a^2}{4}$ 爲有理數,故爲有理整數,於是得到

$$\Delta\equiv a^2\equiv 0 \text{ 或 } 1 \pmod 4.$$

今考慮二次域 $R(\sqrt{D})$, D 爲一無平方因子的有理整數. $R(\sqrt{D})$ 中任意一數均能表成

$$\alpha=\frac{a+b\sqrt{D}}{2}$$

的形式,其中 a, b 爲有理數. α 的跡與距各爲

$$S(\alpha)=a, \qquad N(\alpha)=\frac{a^2-b^2D}{4}.$$

定理 5. 二次域 $R(\sqrt{D})$ 中, α 爲整數的必要且充分之條件爲 a, b 都是有理整數,且適合

$$a\equiv b \pmod 2, \text{ 當 } D\equiv 1 \pmod 4 \text{ 時};$$
$$a\equiv b\equiv 0 \pmod 2, \text{ 當 } D\equiv 2,3 \pmod 4 \text{ 時}. \tag{4}$$

證: 因在二次域中, α 爲整數的充分必要條件爲 $S(\alpha)$, $N(\alpha)$ 全爲有理整數,故若 a, b 全爲有理整數,且 (4) 式成立,則 α 爲整數.

反之,若 α 爲整數,則

$$a \text{ 及 } \frac{a^2-b^2D}{4}$$

爲有理整數,於是

$$b^2D=a^2-4\left(\frac{a^2-b^2D}{4}\right)$$

亦然,但 D 爲無平方因子的有理整數,故 b 必須爲有理整數. 又由

$$a^2-b^2D\equiv 0 \pmod 4,$$

可以很容易地導出 (4) 式,於是定理得證.

故當 $D\equiv 1 \pmod 4$ 時, $\frac{1+\sqrt{D}}{2}$ 爲整數,而有

$$\frac{a+b\sqrt{D}}{2}=\frac{a-b}{2}+b\frac{1+\sqrt{D}}{2},$$

再因

$$\begin{vmatrix} 1 & 1 \\ \sqrt{D} & -\sqrt{D} \end{vmatrix}^2=4D, \qquad \begin{vmatrix} 1 & 1 \\ \frac{1+\sqrt{D}}{2} & \frac{1-\sqrt{D}}{2} \end{vmatrix}^2=D,$$

於是得到:

定理 6. 若 D 爲一無平方因子的有理整數,命

$$\Delta=\begin{cases} D \\ 4D \end{cases},\quad \omega=\begin{cases} \frac{1+\sqrt{D}}{2} \\ \sqrt{D} \end{cases},\quad 當\quad \begin{matrix} D\equiv 1 \pmod 4, \\ D\equiv 2,3 \pmod 4, \end{matrix}$$

則 Δ 爲 $R(\sqrt{D})$ 的基數,而 $1, \omega$ 爲一組整底. 又

$$1, \frac{\Delta+\sqrt{\Delta}}{2}$$

亦爲 $R(\sqrt{D})$ 的一組整底.

由定理 6 可以看到在二次域中恆能找到一整數 ω, 使 $1, \omega$ 爲域的整底,但在一般的情形,亦卽在 n 次域 $R(\vartheta)$ 中 $(n\geqslant 3)$,未必能選出整數 ω, 使

$$1, \omega, \cdots, \omega^{n-1}$$

構成 $R(\vartheta)$ 的整底.

例. 命 α 爲

$$f(x)=x^3-x^2-2x-8=0$$

的根,今將證明在域 $R(\alpha)$ 中决不能找到整數 ω, 使 $1, \omega, \omega^2$ 爲其整底.

因 $\pm 1, \pm 2, \pm 4, \pm 8$, 均非 $f(x)=0$ 的根,故 $f(x)$ 爲不可化,而 $R(\alpha)$ 確爲三次域. 又易證

$$\Delta(1, \alpha, \alpha^2)=-4\cdot 503.$$

因 $\beta=\frac{4}{\alpha}$ 適合方程式

$$g(y)=y^3+y^2+2y-8=0,$$

故 β 爲 $R(\alpha)$ 中之整數. 若以 α', α'' 表 $f(x)=0$ 的另外二根,則

$$\Delta(1, \alpha, \beta)=\begin{vmatrix} 1 & \alpha & 4/\alpha \\ 1 & \alpha' & 4/\alpha' \\ 1 & \alpha'' & 4/\alpha'' \end{vmatrix}^2=\frac{4^2}{(N(\alpha))^2}\begin{vmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha' & \alpha'^2 \\ 1 & \alpha'' & \alpha''^2 \end{vmatrix}^2=$$

$$=\frac{4^2}{(N(\alpha))^2}\Delta(1, \alpha, \alpha^2)=-503.$$

因 $\Delta(1, \alpha, \beta)\neq 0$, 故 $1, \alpha, \beta$ 爲 $R(\alpha)$ 的基底. 又 $1, \alpha, \beta$ 必爲 $R(\alpha)$ 的一組整底,蓋若不然,命 Δ 爲域的基數,則必 $|\Delta|<503$, 由上節 (1) 式,可知必有一不等於 1 的自然數 a, 使

$$-503 = a^2 \Delta,$$

但 503 爲一素數,故不可能,所以 $1, \alpha, \beta$ 必爲域 $R(\alpha)$ 的一組整底.

命 ω 爲 $R(\alpha)$ 內任一整數,則有有理整數 a, b, c 使

$$\omega = a + b\alpha + c\beta.$$

因

$$\alpha^2 = \alpha + 2 + \frac{8}{\alpha} = 2 + \alpha + 2\beta,$$

$$\beta^2 = -\beta - 2 + \frac{8}{\beta} = -2 + 2\alpha - \beta,$$

所以

$$\omega^2 = a^2 + b^2(2 + \alpha + 2\beta) + c^2(-2 + 2\alpha - \beta) + 2ab\alpha + 8bc + 2ac\beta =$$
$$= (a^2 + 2b^2 - 2c^2 + 8bc) + (b^2 + 2c^2 + 2ab)\alpha + (2b^2 - c^2 + 2ac)\beta,$$

因此

$$\Delta(1, \omega, \omega^2) = \begin{vmatrix} 1 & a & a^2 + 2b^2 - 2c^2 + 8bc \\ 0 & b & b^2 + 2c^2 + 2ab \\ 0 & c & 2b^2 - c^2 + 2ac \end{vmatrix}^2 \cdot \Delta(1, \alpha, \beta) \equiv$$
$$\equiv 0 \pmod{4 \cdot 503},$$

所以不論 ω 爲 $R(\alpha)$ 中任何整數,

$$1, \omega, \omega^2$$

不能爲 $R(\alpha)$ 的整底.

§5. 整除性.

定義 1. 設 α, β 爲二整數,若有一整數 γ, 使 $\alpha = \beta\gamma$, 則謂之 β 可整除 α, 並以 $\beta|\alpha$ 記之. 或稱 α 是 β 的倍數, β 是 α 的因子.

定理 1. 命

$$g(x) = \alpha_l x^l + \cdots + \alpha_0, \quad \alpha_l \neq 0,$$
$$h(x) = \beta_m x^m + \cdots + \beta_0, \quad \beta_m \neq 0,$$

此處諸 α 及 β 都是整數. 又命

$$g(x)\, h(x) = \gamma_{l+m} x^{l+m} + \cdots + \gamma_0,$$

若有一整數 δ 適合

$$\delta \mid \gamma_u \quad (0 \leqslant u \leqslant l + m), \tag{1}$$

則必有

$$\delta \mid \alpha_v \beta_w \qquad (0 \leqslant v \leqslant l, \quad 0 \leqslant w \leqslant m). \tag{2}$$

定理之證明有賴於次之二引.

引 1. 若

$$f(x) = \delta_n x^n + \cdots + \delta_0, \quad n \geqslant 1 \tag{3}$$

是一整係數的多項式,且有一根 μ, 則

$$\frac{f(x)}{x-\mu}$$

也有整係數.

證: 當 $n=1$ 時, $\mu = -\frac{\delta_0}{\delta_1}$, $\frac{f(x)}{x-\mu} = \delta_1$ 爲一整數,而引理成立.

今於 n 上施行歸納法,假定本引理對 $n-1$ 次多項式眞實,由於 $\delta_n \mu$ 適合

$$y^n + \cdots + \delta_1 \delta_n^{n-2} y + \delta_0 \delta_n^{n-1} = 0,$$

故 $\delta_n \mu$ 爲一整數 (本章 §1 習題 2). 所以

$$g(x) = f(x) - (x-\mu)\delta_n x^{n-1} = (f(x) - \delta_n x^n) + \delta_n \mu x^{n-1}$$

爲一次數不大於 $n-1$ 的整係數多項式, 且有 μ 爲其根. 故由數學歸納法的假定,有整係數多項式 $h(x)$,使

$$g(x) = (x-\mu) h(x),$$

於是

$$f(x) = (x-\mu)(\delta_n x^{n-1} + h(x)),$$

引理得證.

引 2. 命 $\mu_1, \cdots, \mu_r$ $(1 \leqslant r \leqslant n)$ 爲 (3) 式任意 r 個根,則

$$\delta_n \mu_1 \cdots \mu_r$$

是整數.

證: 因

$$f(x) = \delta_n (x-\mu_1) \cdots (x-\mu_r) \cdots (x-\mu_n),$$

應用引 1, 可知

$$\frac{f(x)}{x-\mu_n}, \frac{f(x)}{(x-\mu_{n-1})(x-\mu_n)}, \cdots, \frac{f(x)}{(x-\mu_{r+1})\cdots(x-\mu_n)} = \delta_n (x-\mu_1)\cdots(x-\mu_r)$$

皆爲有整係數的多項式,故得證.

定理 1 之證明: 若 $l=0$ 或 $m=0$, 定理顯然眞實,故不妨假定 $l>0$ 及 $m>0$ 而討論之. 將 $g(x)$ 及 $h(x)$ 分解成

$$g(x)=\alpha_l(x-\xi_1)\cdots(x-\xi_l),$$
$$h(x)=\beta_m(x-\eta_1)\cdots(x-\eta_m),$$

則得

$$\frac{g(x)\,h(x)}{\delta}=\frac{\alpha_l\,\beta_m}{\delta}(x-\xi_1)\cdots(x-\xi_l)(x-\eta_1)\cdots(x-\eta_m)$$

為整係數多項式．若命 $\sigma_0=\tau_0=1$, $\sigma_1,\cdots,\sigma_l$ 與 $\tau_1,\cdots,\tau_m$ 分別為 $\xi_1,\cdots,\xi_l$ 及 $\eta_1,\cdots,\eta_m$ 的初等對稱多項式．則由引 2，可以推得對任何 $0\leqslant v\leqslant l$, $0\leqslant w\leqslant m$ 中之 v, w,

$$\frac{\alpha_l\,\beta_m}{\delta}\sigma_{l-v}\,\tau_{m-w}$$

皆為整數．再由多項式的根與係數之關係，

$$\alpha_v=\pm\,\alpha_l\,\sigma_{l-v},$$
$$\beta_w=\pm\,\beta_m\,\tau_{m-w},$$

於是

$$\frac{\alpha_v\,\beta_w}{\delta}=\pm\frac{\alpha_l\,\beta_m}{\delta}\sigma_{l-v}\,\tau_{m-w}$$

為整數．

由整除性十分自然地會聯想到代數整數之因子分解定理及其唯一性的問題．

但在全體代數整數的範圍內，討論因子分解是沒有意義的，因為一個整數可能表示為無限多個整數的乘積．例如

$$2=2^{1/2}\cdot 2^{1/4}\cdot 2^{1/8}\cdots,$$

此點提示我們必須限定因子所在的範圍．所以我們僅討論在某一代數數域$R(\vartheta)$內的整數分解的問題．

但在一代數數域內可能有無窮多個單位數．設 ε 為一單位數，則任一整數可表示為

$$\alpha=\varepsilon\cdot\varepsilon^{-1}\alpha.$$

因此若 $R(\vartheta)$ 內有無窮多個單位數，則 α 可能有無窮多個分解方法．例如在 $R(\sqrt{2})$ 中 $(1+\sqrt{2})^n$ $(n=\pm1,\pm2,\cdots)$ 都是單位數，所以 $R(\sqrt{2})$ 中的整數就可能有無窮多種分解法．為了避免這個問題，我們引進"結合"的定義．

定義 2. 若二整數 α,β 僅相差一單位因子，則 α 與 β 稱為相結合．

顯然有次之三性質：1) α 與 α 相結合；2) 若 α 與 β 相結合，則 β 與 α

相結合; 3) 若 α 與 β 相結合, β 與 γ 相結合, 則 α 與 γ 相結合.

定義 3. 對於整數 α, 若有 $R(\vartheta)$ 中的整數 β, γ, 且均非單位數,使

$$\alpha = \beta\gamma,$$

則稱 α 在 $R(\vartheta)$ 中可分解,否則稱爲不可分解.

定理 2. 在 $R(\vartheta)$ 中任一代數整數可以分解爲不可分解的代數整數的乘積.

證: 若 α 不可分解,則定理毋待證明. 若

$$\alpha = \beta\gamma,$$

而 β, γ 均非單位數,則得

$$|N(\alpha)| = |N(\beta)| \cdot |N(\gamma)|,$$

由於 β, γ 均非單位數,故自然數 $|N(\beta)|, |N(\gamma)|$ 爲 $|N(\alpha)|$ 的眞因子,即

$$|N(\alpha)| > |N(\beta)| > 1, \qquad |N(\alpha)| > |N(\gamma)| > 1.$$

故可用對 $|N(\alpha)|$ 施行歸納法而證明本定理.

餘下的問題是分解的方法是否唯一的問題, 此乃代數數論的一個重要問題. 今具體的考察二次域 $R(\sqrt{-5})$, 我們將證明在此域內唯一分解的性質不成立.

因 $-5 \equiv 3 \pmod{4}$, 故此域内之整數都是次之形式:

$$\alpha = a + b\sqrt{-5},$$

其中 a, b 都是有理整數. 今將證明在此域內, $2, 3, 1 \pm \sqrt{-5}$ 都不可分解,且 $2, 3$ 不能與 $1+\sqrt{-5}$, $1-\sqrt{-5}$ 相結合,於是由

$$6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

可知在 $R(\sqrt{-5})$ 中唯一分解定理不能成立.

因

$$|N(2)| = 4, |N(3)| = 9, \qquad |N(1 \pm \sqrt{-5})| = 6,$$

故 $2, 3$ 不能與 $1+\sqrt{-5}$, $1-\sqrt{-5}$ 相結合.

又若 2 在 $R(\sqrt{-5})$ 中可分解,命

$$2 = \alpha\beta, \quad |N(\alpha)| > 1, \quad |N(\beta)| > 1,$$

記 $\alpha = a + b\sqrt{-5}$，則因 $|N(2)| = 4$，故必須

$$|N(\alpha)| = a^2 + 5b^2 = 2,$$

但此乃不可能之事，故在 $R(\sqrt{-5})$ 中 2 不能分解，同樣可證 3, $1 \pm \sqrt{-5}$ 在 $R(\sqrt{-5})$ 中不可分解.

爲了解決這一問題，Kummer 氏發明了理想數的概念.

§ 6. **理想數**. 今確定一 n 次的代數數域 $R(\vartheta)$ 作爲基礎.

定義 1. 命 $\alpha_1, \cdots, \alpha_q$ 爲 $R(\vartheta)$ 內任意 q 個整數. 稱所有形如

$$\eta_1 \alpha_1 + \cdots + \eta_q \alpha_q \quad (\eta_1, \cdots, \eta_q \text{ 爲 } R(\vartheta) \text{ 中的整數}) \tag{1}$$

的整數所成之集合爲由 $\alpha_1, \cdots, \alpha_q$ 演成的理想數，以 $[\alpha_1, \cdots, \alpha_q]$ 表之.

爲簡單起見，在今後討論理想數的一般性質時，常以德文大寫字母 $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, … 來表示理想數.

定義 2. 由一個整數 α 所演成之理想數 $[\alpha]$，稱爲主理想數.

祗有一個整數 0 所成的集合，亦成一理想數 $[0]$. 今假定以後所討論之理想數，均非 $[0]$.

理想數 $[1]$ 表示由 $R(\vartheta)$ 內全體整數所成的集合，稱爲單位理想數，以 $\mathfrak{O}$ 表之.

定理 1. 理想數有次之性質：

1) 若 α, β 在其中，則 $\alpha \pm \beta$ 亦然，

2) 若 α 在此集合中，而 η 爲 $R(\vartheta)$ 中的任一整數，則 $\eta\alpha$ 也在此理想數中.

證：其理顯然.

由此定理，若理想數 $\mathfrak{A}$ 中包有 1，則 $\mathfrak{A}$ 中包有 $R(\vartheta)$ 內的全體整數，所以 $\mathfrak{A} = [1]$.

定義 3. 設 $\mathfrak{A} = [\alpha_1, \cdots, \alpha_q]$ 及 $\mathfrak{B} = [\beta_1, \cdots, \beta_r]$ 爲 $R(\vartheta)$ 上的二理想數，當 $\mathfrak{A}$ 中每一整數均在 $\mathfrak{B}$ 中，而 $\mathfrak{B}$ 中每一整數又均在 $\mathfrak{A}$ 中時，則稱它們爲相等，並記 $\mathfrak{A} = \mathfrak{B}$.

由此定義立得：

定理 2. 二理想數 $\mathfrak{A} = [\alpha_1, \cdots, \alpha_q]$, $\mathfrak{B} = [\beta_1, \cdots, \beta_r]$ 相等的必要且充分

之條件爲

$$\alpha_i=\sum_{j=1}^{r}\xi_{ij}\,\beta_j,\quad \beta_j=\sum_{i=1}^{q}\eta_{ji}\,\alpha_i,\tag{2}$$

其中 $1\leqslant i\leqslant q$, $1\leqslant j\leqslant r$, 而諸 ξ 及 η 均爲整數. 更由此可得: 若 $[\alpha]=$ $=[\beta]$, 則 α 與 β 爲相結合.

設 $a_1,\cdots,a_q$ 爲任意 q 個有理整數, d 爲他們的最大公約數, 則由最大公約數的性質, 必有有理整數 $x_1,\cdots,x_q$ 使

$$d=a_1\,x_1+\cdots+a_q\,x_q,$$

所以在有理數域中 $[a_1,\cdots,a_q]=[d]$, 亦即在有理數域中, 祇有主理想數存在.

但若考慮域 $R(\sqrt{-5})$, 由上節最後之討論, 可知理想數 $[2,1+\sqrt{-5}]$ 決不能化爲主理想數, 所以有非主理想數的理想數存在.

定義 4. 理想數

$$[\alpha_1\,\beta_1,\cdots,\alpha_1\,\beta_r,\alpha_2\,\beta_1,\cdots,\alpha_2\,\beta_r\cdots,\alpha_q\,\beta_r]$$

稱爲理想數

$$\mathfrak{A}=[\alpha_1,\cdots,\alpha_q]\quad 及\quad \mathfrak{B}=[\beta_1,\cdots,\beta_r]$$

的乘積, 以 $\mathfrak{A}\cdot\mathfrak{B}$ 記之.

定理 3. $\mathfrak{A}$ 與 $\mathfrak{B}$ 之乘積與諸 α 及 β 之選擇無關, 亦卽, 若

$$\mathfrak{A}=[\alpha_1,\cdots,\alpha_q]=[\alpha_1',\cdots,\alpha_s'],$$

$$\mathfrak{B}=[\beta_1,\cdots,\beta_r]=[\beta_1',\cdots,\beta_t'],$$

則

$$\mathfrak{A}\cdot\mathfrak{B}=[\alpha_1\,\beta_1,\cdots,\alpha_1\,\beta_r,\alpha_2\,\beta_1,\cdots,\alpha_2\,\beta_r,\cdots,\alpha_q\,\beta_r]=$$
$$=[\alpha_1'\,\beta_1',\cdots,\alpha_1'\,\beta_t',\alpha_2'\,\beta_1',\cdots,\alpha_2'\,\beta_t',\cdots,\alpha_s'\,\beta_t'].$$

證明可以很容易地從理想數相等的定義得到, 讀者自證之.

易見對任何理想數 $\mathfrak{A}$, 有 $\mathfrak{O}\cdot\mathfrak{A}=\mathfrak{A}$.

由乘法定義, 不難證明:

1) 交換律 $\mathfrak{A}\cdot\mathfrak{B}=\mathfrak{B}\cdot\mathfrak{A}$;

2) 結合律 $(\mathfrak{A}\cdot\mathfrak{B})\cdot\mathfrak{C}=\mathfrak{A}\cdot(\mathfrak{B}\cdot\mathfrak{C})$.

因此可用歸納法定義 $\mathfrak{A}_1\cdots\mathfrak{A}_m=(\mathfrak{A}_1\cdots\mathfrak{A}_{m-1})\cdot\mathfrak{A}_m$, 及 $\mathfrak{A}^m=\mathfrak{A}^{m-1}\cdot\mathfrak{A}$ (m 爲任

何自然數);並定義對任何理想數 $\mathfrak{A}$, $\mathfrak{A}^0=\mathfrak{O}$. 於是易證下列諸性質:

$$\mathfrak{A}^m\cdot\mathfrak{A}^l=\mathfrak{A}^{m+l},$$
$$(\mathfrak{A}^l)^m=\mathfrak{A}^{lm},$$
$$(\mathfrak{A}\cdot\mathfrak{B})^m=\mathfrak{A}^m\cdot\mathfrak{B}^m.$$

定義 5. 命 $\mathfrak{A}$, $\mathfrak{B}$ 是二理想數,若有理想數 $\mathfrak{C}$ 使

$$\mathfrak{A}=\mathfrak{B}\cdot\mathfrak{C},$$

則謂之 $\mathfrak{B}$ 可整除 $\mathfrak{A}$, 記如 $\mathfrak{B}|\mathfrak{A}$. $\mathfrak{B}$, $\mathfrak{C}$ 稱爲 $\mathfrak{A}$ 之因子.

顯然有:

1) 若 $\mathfrak{C}|\mathfrak{B}$, $\mathfrak{B}|\mathfrak{A}$, 則 $\mathfrak{C}|\mathfrak{A}$,

2) 若 $\mathfrak{B}|\mathfrak{A}$, 而 $\mathfrak{D}$ 爲任何理想數,則 $\mathfrak{B}\mathfrak{D}|\mathfrak{A}\mathfrak{D}$,

3) 對任何理想數 $\mathfrak{A}$, 有

$$\mathfrak{O}\mid\mathfrak{A},\qquad \mathfrak{A}\mid\mathfrak{A}.$$

定理 4. 若 $\mathfrak{B}|\mathfrak{A}$, 則 $\mathfrak{A}$ 中任一整數都在 $\mathfrak{B}$ 中.

證: 命 $\mathfrak{A}=\mathfrak{B}\cdot\mathfrak{C}$, 而 $\mathfrak{B}=[\beta_1,\cdots,\beta_r]$, $\mathfrak{C}=[\gamma_1,\cdots,\gamma_s]$. 則凡 $\mathfrak{A}$ 中之數 α 皆爲

$$\alpha=\sum_{j=1}^{r}\sum_{k=1}^{s}\eta_{jk}\beta_j\gamma_k=\sum_{j=1}^{r}\left(\sum_{k=1}^{s}\eta_{jk}\gamma_k\right)\beta_j$$

之形式,其中 η_{jk} 爲域中之整數,故 α 在 $\mathfrak{B}$ 中,定理得證.

在下節中將證明定理 4 之逆亦成立,卽若 $\mathfrak{A}$ 中任一整數都在 $\mathfrak{B}$ 中時,則必 $\mathfrak{B}|\mathfrak{A}$.

由定理 4 可得: 若 $\mathfrak{A}|\mathfrak{O}$, 則 $\mathfrak{A}=\mathfrak{O}$.

§ 7. 理想數的唯一分解定理.

定理 1. 對於任何理想數 $\mathfrak{A}$ 一定能找到一個理想數 $\mathfrak{B}$, 使 $\mathfrak{A}$,$\mathfrak{B}$ 的乘積爲一由一自然數 a 演成的主理想數 $[a]$.

證: 若 $\mathfrak{A}$ 爲一主理想數如 $\mathfrak{A}=[\alpha]$, 則取 $\mathfrak{B}=[\alpha^{(2)}\cdots\alpha^{(n)}]$, $\alpha^{(2)},\cdots,\alpha^{(n)}$ 爲 α 的共軛數,於是取 $a=|N(\alpha)|$,立得

$$\mathfrak{A}\cdot\mathfrak{B}=[\alpha\,\alpha^{(2)}\cdots\alpha^{(n)}]=[a].$$

若 $\mathfrak{A}$ 非主理想數,命 $\mathfrak{A}=[\alpha_l,\cdots,\alpha_0]$, 作多項式

$$f(x)=\alpha_l x^l+\cdots+\alpha_0.$$

又命

$$g(x)=\beta_m x^m+\cdots+\beta_0 \qquad (m=(n-1)\,l)$$

適合

$$f(x)\,g(x)=\prod_{j=1}^{n}(\alpha_l^{(j)}x^l+\cdots+\alpha_0^{(j)})=$$
$$=c_{l+m}x^{l+m}+\cdots+c_0,$$

其中諸 c 都是有理整數,於是諸 β 也均爲 $R(\vartheta)$ 中的整數. 命

$$\mathfrak{B}=[\beta_m,\cdots,\beta_0]$$

及

$$a=(c_{l+m},\cdots,c_0),$$

今往證明

$$\mathfrak{A}\cdot\mathfrak{B}=[a].$$

因對所有 $0\leqslant k\leqslant l+m$, 有

$$a\mid c_k,$$

於是由定理 5.1, 可得

$$a\mid\alpha_\mu\beta_\nu \qquad (0\leqslant\mu\leqslant l,\ \ 0\leqslant\nu\leqslant m),$$

所以 $\alpha_\mu\beta_\nu$ 皆在 $[a]$ 中. 反之,因 $a=(c_{l+m},\cdots,c_0)$,故有有理整數 $d_{l+m},\cdots,d_0$,使

$$a=c_{l+m}d_{l+m}+\cdots+c_0d_0.$$

又因

$$c_k=\sum_{\substack{\mu+\nu=k\\0\leqslant\mu\leqslant l\\0\leqslant\nu\leqslant m}}\alpha_\mu\beta_\nu \qquad (0\leqslant k\leqslant l+m),$$

故有

$$a=\sum_{\mu=1}^{l}\sum_{\nu=1}^{m}\eta_{\mu\nu}\alpha_\mu\beta_\nu,$$

其中諸 η 皆爲 $R(\vartheta)$ 中的整數,所以 a 在 $\mathfrak{A}\cdot\mathfrak{B}$ 中. 因此

$$\mathfrak{A}\cdot\mathfrak{B}=[a].$$

定理 2. 若 $\mathfrak{A}\cdot\mathfrak{C}=\mathfrak{A}\cdot\mathfrak{D}$, 則必 $\mathfrak{C}=\mathfrak{D}$.

證: 取 $\mathfrak{B}$ 及自然數 a, 使

$$\mathfrak{A}\cdot\mathfrak{B}=[a].$$

於是有

$$[a]\cdot\mathfrak{C} = [a]\cdot\mathfrak{D},$$

此等式之意義爲由 $\mathfrak{C}$ 中各數乘以 a 後所得之集合與由 $\mathfrak{D}$ 中各數乘以 a 後所得之集合相同,所以得到

$$\mathfrak{C} = \mathfrak{D}.$$

定理 3. 若理想數 $\mathfrak{C}$ 中每一元素均在另一理想數 $\mathfrak{A}$ 中時,則必

$$\mathfrak{A} \mid \mathfrak{C}.$$

證: 取 $\mathfrak{B}$ 及 a 使

$$\mathfrak{A}\cdot\mathfrak{B} = [a],$$

於是 $\mathfrak{B}\cdot\mathfrak{C}$ 中每一元素均在 $\mathfrak{A}\cdot\mathfrak{B} = [a]$ 中,故可命

$$\mathfrak{B}\cdot\mathfrak{C} = [a\gamma_1, \cdots, a\gamma_q] = [a]\cdot[\gamma_1, \cdots, \gamma_q] =$$
$$= \mathfrak{B}\cdot\mathfrak{A}\cdot[\gamma_1, \cdots, \gamma_q],$$

而得

$$\mathfrak{C} = \mathfrak{A}\cdot[\gamma_1, \cdots, \gamma_q],$$

定理得證.

由本定理及定理 6.4 可知 $\mathfrak{B}|\mathfrak{A}$ 的必要且充分之條件爲 $\mathfrak{A}$ 中每一元素均在 $\mathfrak{B}$ 中.

今往討論理想數的分解及其唯一性的問題.

定義 1. 若一理想數祇有二個因子,卽除了 $\mathfrak{O}$ 及其本身以外别無其他因子者稱爲素理想數. 通常以 $\mathfrak{P}$ 表示素理想數.

易證在有理數域中 $[p]$ 爲素理想數,其中 p 爲普通的有理素數.

定理 4. 任與二理想數 $\mathfrak{A} = [\alpha_1, \cdots, \alpha_q]$, $\mathfrak{B} = [\beta_1, \cdots, \beta_r]$, 則有唯一的理想數 $\mathfrak{D}$ 具有次之性質:

1) $\mathfrak{D}|\mathfrak{A}$, $\mathfrak{D}|\mathfrak{B}$;

2) 若另有一理想數 $\mathfrak{D}_1$, $\mathfrak{D}_1|\mathfrak{A}$, $\mathfrak{D}_1|\mathfrak{B}$, 則 $\mathfrak{D}_1|\mathfrak{D}$.

更可言者,$\mathfrak{D}$ 中任何一數都能寫成 $\alpha+\beta$ 的形式, α 在 $\mathfrak{A}$ 中, β 在 $\mathfrak{B}$ 中.

證: $\mathfrak{D} = [\alpha_1, \cdots, \alpha_q, \beta_1, \cdots, \beta_r]$ 卽有上述諸性質.

顯然有 $\mathfrak{D}|\mathfrak{A}$, $\mathfrak{D}|\mathfrak{B}$. 又若有理想數 $\mathfrak{D}_1|\mathfrak{A}$, $\mathfrak{D}_1|\mathfrak{B}$, 則 $\mathfrak{D}_1$ 包有 $\mathfrak{A}$ 及 $\mathfrak{B}$, 故亦包有 $\mathfrak{D}$, 所以有 $\mathfrak{D}_1]\mathfrak{D}$.

再證明 $\mathfrak{D}$ 之唯一性. 若 $\mathfrak{D}'$ 也具有 1), 2) 二性質,則

$$\mathfrak{D}' \mid \mathfrak{D}, \quad \mathfrak{D} \mid \mathfrak{D}',$$

亦卽 $\mathfrak{D}$ 中各數均在 $\mathfrak{D}'$ 中,而 $\mathfrak{D}'$ 中各數也均在 $\mathfrak{D}$ 中,所以

$$\mathfrak{D}' = \mathfrak{D}.$$

又因 $\mathfrak{D} = [\alpha_1, \cdots, \alpha_q, \beta_1, \cdots, \beta_r]$ 中任何一數都能寫成

$$\eta_1 \alpha_1 + \cdot + \eta_q \alpha_q + \lambda_1 \beta_1 + \quad + \lambda_r \beta_r$$

的形式. 命 $\alpha = \eta_1\alpha_1 + \cdots + \eta_q \eta_q$, $\beta = \lambda_1 \beta_1 + \cdots + \lambda_r \beta_r$, 則 α 在 $\mathfrak{A}$ 中, β 在 $\mathfrak{B}$ 中,因此 $\mathfrak{D}$ 中任一元素都能表成 $\alpha + \beta$ 的形式.

定義 2. 定理 4 中的 $\mathfrak{D}$ 稱爲 $\mathfrak{A}, \mathfrak{B}$ 的最大公因子,以 $\mathfrak{D} = (\mathfrak{A}, \mathfrak{B})$ 記之,更可定義 $(\mathfrak{A}_1, \cdots, \mathfrak{A}_{m-1}, \mathfrak{A}_m) = ((\mathfrak{A}_1, \cdots, \mathfrak{A}_{m-1}), \mathfrak{A}_m)$. 若 $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{O}$, 則稱 $\mathfrak{A}, \mathfrak{B}$ 爲互素.

易證: 若 $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{D}$, 則對任何理想數 $\mathfrak{C}$, 有

$$(\mathfrak{A}\mathfrak{C}, \mathfrak{B}\mathfrak{C}) = \mathfrak{D}\mathfrak{C}.$$

定理 5. 若 $\mathfrak{P}$ 爲一素理想數,且 $\mathfrak{P} \mid \mathfrak{A}\mathfrak{B}$, $\mathfrak{P} \nmid \mathfrak{A}$, 則 $\mathfrak{P} \mid \mathfrak{B}$.

證: 因 $\mathfrak{P} \nmid \mathfrak{A}$, 所以

$$(\mathfrak{P}, \mathfrak{A}) = \mathfrak{O},$$

於是

$$(\mathfrak{P}\mathfrak{B}, \mathfrak{A}\mathfrak{B}) = \mathfrak{B},$$

又因 $\mathfrak{P} \mid \mathfrak{A}\mathfrak{B}$, 所以 $\mathfrak{P} \mid \mathfrak{B}$.

定理 6. 任何理想數都祗能有有限個不同的因子.

證: 對於 $\mathfrak{A}$ 有理想數 $\mathfrak{B}$ 及自然數 a, 使

$$\mathfrak{A} \cdot \mathfrak{B} = [a],$$

故 $\mathfrak{A}$ 中含有 a, 且 $\mathfrak{A}$ 之任何因子亦含有 a, 故若能證明含有一個固定的自然數的理想數,祗可能有有限個,則定理明矣.

設 $\mathfrak{M} = [\alpha_1, \cdots, \alpha_m]$ 爲一含有 a 的理想數. 又設 $\omega_1, \cdots, \omega_n$ 爲 $R(\mathfrak{I})$ 的一組整底,於是諸 α 能表成下列形式:

$$\alpha_j = g_{j1}\, \omega_1 + \cdots + g_{jn}\, \omega_n \qquad (1 \leqslant j \leqslant m),$$

其中諸 g 爲有理整數. 再令

$$g_{ik} = a\,q_{ik} + r_{ik} \qquad (0 \leqslant r_{ik} < a),$$

$$\beta_i = \sum_{k=1}^{n} q_{ik}\,\omega_k, \qquad \gamma_i = \sum_{k=1}^{n} r_{ik}\,\omega_k,$$

於是得到

$$\alpha_i = a\beta_i + \gamma_i.$$

又因 a 在 $\mathfrak{M}$ 中,所以

$$\mathfrak{M} = [a\beta_1 + \gamma_1, \cdots, a\beta_m + \gamma_m, a] =$$
$$= [\gamma_1, \cdots, \gamma_m, a].$$

因爲祇有有限組 $\gamma_1, \cdots, \gamma_m$, 故含有 a 的理想數,祇可能爲有限個.

定理 7 (理想數之基本定理). 任一不同於 $\mathfrak{O}$ 的理想數 $\mathfrak{A}$ 可以分解爲素理想數的乘積,且若不計其排列之次序,則分解法唯一.

證: 因爲任何理想數祇可能有有限多個不同的因子,故可對 $\mathfrak{A}$ 的因子個數實行數學歸納法.

先證明分解之可能. 若 $\mathfrak{A}$ 已爲素理想數,則毋需再證;若不然,而

$$\mathfrak{A} = \mathfrak{B}\mathfrak{C} \quad (\mathfrak{B} \neq \mathfrak{O}, \mathfrak{C} \neq \mathfrak{O}),$$

則因 $\mathfrak{B}, \mathfrak{C}$ 的因子個數少於 $\mathfrak{A}$ 的因子個數,故由數學歸納法,得到證明.

再證分解的唯一性. 假定

$$\mathfrak{A} = \mathfrak{P}_1 \mathfrak{P}_2 \cdots \mathfrak{P}_l = \mathfrak{P}_1' \mathfrak{P}_2' \cdots \mathfrak{P}_m', \quad m \geqslant 1, \quad l \geqslant 1. \tag{1}$$

若 $\mathfrak{A}$ 是素理想數, 則 $l = m = 1$. 毋待證明. 若 $\mathfrak{A}$ 非素理想數, 則 $l > 1$, $m > 1$. 因

$$\mathfrak{P}_1 \mid \mathfrak{P}_1' \cdots \mathfrak{P}_m',$$

故必有一 $\mathfrak{P}_j'$ $(1 \leqslant j \leqslant m)$ 使 $\mathfrak{P}_1 = \mathfrak{P}_j'$. 不失普遍性地可以假定 $j = 1$. 於是

$$\mathfrak{P}_2 \cdots \mathfrak{P}_l = \mathfrak{P}_2' \cdots \mathfrak{P}_m',$$

由數學歸納法假定,定理得證.

因此可將任一不同於 $\mathfrak{O}$ 的理想數表爲

$$\mathfrak{P}_1^{a_1} \mathfrak{P}_2^{a_2} \cdots \mathfrak{P}_r^{a_r}$$

的形式,其中諸 $\mathfrak{P}$ 各各不同, a_i 爲自然數. 又若不計諸 $\mathfrak{P}$ 之次序, 則這種表法是唯一的.

習題 1. 任與二理想數 $\mathfrak{A}$ 及 $\mathfrak{B}$, 必有一整數 α, 使 $\mathfrak{A}|[\alpha]$, 且 $([\alpha], \mathfrak{A}\mathfrak{B})=\mathfrak{A}$.

習題 2. 任何理想數 $\mathfrak{A}$ 皆能表為 $[\alpha, \beta]$ 的形式, α, β 皆為整數, 且 β 可取為 $\mathfrak{A}$ 中任何整數 (在習題 1 中取 $\mathfrak{B}$, $[\beta]$ 使適合 $\mathfrak{A}\mathfrak{B} = [\beta]$).

§ 8. 理想數的基底.

設 $\omega_1, \cdots, \omega_n$ 為域 $R(\vartheta)$ 的一組整底,而 $\mathfrak{A}$ 為 $R(\vartheta)$ 上的任一理想數. 因 $\mathfrak{A}$ 中任一元素都能表為 $\omega_1, \cdots, \omega_n$ 的係數是有理整數的線性組合,再由定理 6.1, 故能將 $\mathfrak{A}$ 看作 $\omega_1, \cdots, \omega_n$ 的一個線性模. 又對理想數 $\mathfrak{A}$, 必有理想數 $\mathfrak{B}$ 及自然數 a, 使

$$\mathfrak{A}\mathfrak{B} = [a],$$

因此 $a\omega_1, \cdots, a\omega_n$ 都在 $\mathfrak{A}$ 中,而因這 n 個數是線性獨立的,所以 $\mathfrak{A}$ 是 $\omega_1, \cdots, \omega_n$ 的一 n 維線性模. 由第 14 章第 9 節的討論,可知 $\mathfrak{A}$ 必有底,且 $\mathfrak{A}$ 的任何一組基底中都必須含有 n 個整數. 特別的,我們更可得到:

定理 1. 設 $\mathfrak{A}$ 為 $R(\vartheta)$ 上的任何一個理想數, 則在 $\mathfrak{A}$ 中必能找到 n 個整數

$$\alpha_1 = a_{11}\,\omega_1,$$
$$\alpha_2 = a_{21}\,\omega_1 + a_{22}\,\omega_2,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\alpha_n = a_{n1}\,\omega_1 + a_{n2}\,\omega_2 + \cdots + a_{nn}\,\omega_n,$$

其中 a_{ij} 都是有理整數,且 $a_{ii} > 0$ $(1 \leqslant i \leqslant n)$,而 $0 \leqslant a_{ji} < a_{ii}$ $(1 \leqslant i < j \leqslant n)$, 使 $\alpha_1, \cdots, \alpha_n$ 成為 $\mathfrak{A}$ 的標準基底.

又設 $\alpha_1, \cdots, \alpha_n$ 與 $\beta_1, \cdots, \beta_n$ 為 $\mathfrak{A}$ 的二組基底,而命

$$\alpha_i = \sum_{j=1}^{n} u_{ij}\,\beta_j \quad (i = 1, \cdots, n),$$

則其係數矩陣 (u_{ij}) 必為一模方陣,因此

$$\Delta(\alpha_1, \cdots, \alpha_n) = \Delta(\beta_1, \cdots, \beta_n),$$

亦卽理想數基底的判別式不因基底的改變而改變,故今後可以 $\Delta(\mathfrak{A})$ 表之.

今往考慮二次域 $R(\sqrt{D})$ 上理想數的標準基底的形式. 命 $1, \omega$ 為 $R(\sqrt{D})$ 的整底. ω 的定義見定理 4.6. 由定理 1 可以找到二個整數

$$a, \quad b + c\omega$$

組成理想數的標準基底，其中 a, b, c 都是有理整數，且可假定 $a>0$, $c>0$, $0\leqslant b<a$. 但必須注意並非如上形式的任何一對整數，都能成爲某理想數的基底，a, b, c 尙須適合其他條件方可.

易證當且僅當

$$a\omega,\quad \omega(b+c\omega)$$

都能表成

$$xa+y(b+c\omega)\quad (x, y \text{ 爲有理整數})$$

時，$a, b+c\omega$ 才能是某一理想數的標準基底. 從

$$a\omega=xa+y(b+c\omega)$$

可得

$$a=yc,\quad ax+by=0,$$

所以必有 $c|a$, $c|b$. 命

$$a=cm,\quad b=cn.$$

又因

$$c(n+\omega)\,\omega=c(n+\omega)\,(n+\omega+\omega')-c(n+\omega)\,(n+\omega')=$$
$$=-cN(n+\omega)+c(n+\omega)\,(n+S(\omega)),$$

其中 $S(\omega)$ 與 $N(n+\omega)$ 各表示數 ω 與 $n+\omega$ 的跡與矩，所以

$$N(n+\omega)\equiv 0\pmod m \tag{1}$$

乃整數對 cm, $c(n+\omega)$ 成爲某理想數標準基底的充分必要條件. 又由定理 4.6，易見 (1) 式與

$$\Delta\equiv\begin{cases}(2n+1)^2 \pmod{4m}, & \text{若 } D\equiv 1 \pmod 4;\\ (2n)^2 \pmod{4m}, & \text{若 } D\equiv 2,3 \pmod 4\end{cases} \tag{2}$$

等價，於是得到：

定理 2. 整數對 cm, $c(n+\omega)$ $(c>0,\ m>0,\ 0\leqslant n<m)$ 成爲域 $R(\sqrt{D})$ 上某理想數的標準基底的充分必要條件爲 (1) 式或 (2) 式成立.

習題. 令 $\omega_1,\cdots,\omega_n$ 爲 $R(\vartheta)$ 的一組整底，則 $\alpha_i\omega_j$ $(1\leqslant i\leqslant n, 1\leqslant j\leqslant n)$ 能唯一地表成

$$x_1\alpha_1+\cdots+x_n\alpha_n\quad (x_i \text{ 全爲有理整數})$$

之形式乃 $\alpha_1,\cdots,\alpha_n$ 爲某理想數的基底的充分必要條件.

§9. **同餘關係.**

定義 1. 若 $\mathfrak{A}|[\alpha]$, 則謂之 $\mathfrak{A}$ 整除 α, 逕以 $\mathfrak{A}|\alpha$ 表之. 易見 $\mathfrak{A}|\alpha$ 亦卽 α 在 $\mathfrak{A}$ 中的意思.

又根據第 14 章第 9 節的討論,可以定義域 $R(\vartheta)$ 中的整數對理想數 $\mathfrak{A}$ 的同餘關係,具體言之:

定義 2. 若 $\mathfrak{A}|\alpha-\beta$, α, β 爲 $R(\vartheta)$ 中的整數,則謂之 α 與 β 對模 $\mathfrak{A}$ 同餘,記之爲

$$\alpha\equiv\beta \pmod{\mathfrak{A}}.$$

根據此同餘關係,可以將域 $R(\vartheta)$ 中的整數進行分類,使凡屬於同類的數對模 $\mathfrak{A}$ 互相同餘,而屬於不同類的整數不能對模 $\mathfrak{A}$ 同餘. 稱這種類爲 $\mathfrak{A}$ 的剩餘類,並以 $N(\mathfrak{A})$ 表示類數, $N(\mathfrak{A})$ 亦稱爲理想數 $\mathfrak{A}$ 的距. 由定理 14.9.3 可得:

定理 1. 命 $\omega_1, \cdots, \omega_n$ 爲 $R(\vartheta)$ 的一組整底,而 $\alpha_1, \cdots, \alpha_n$ 爲理想數 $\mathfrak{A}$ 的任何一組基底,若

$$\alpha_i=\sum_{j=1}^{n} a_{ij}\,\omega_j,$$

則 $N(\mathfrak{A})$ 等於係數行列式的絕對值,亦卽

$$N(\mathfrak{A})=||a_{ij}||.$$

由此定理,立刻得到:

定理 2. 命 Δ 爲域 $R(\vartheta)$ 的基數, $\Delta(\mathfrak{A})$ 爲 $\mathfrak{A}$ 的基底的判別式,則

$$\Delta(\mathfrak{A})=(N(\mathfrak{A}))^2\,\Delta. \tag{1}$$

及

定理 3. 對於主理想數 $[\alpha]$ 的距 $N([\alpha])$,有

$$N([\alpha])=|N(\alpha)|.$$

證: 設 $\omega_1, \cdots, \omega_n$ 爲 $R(\vartheta)$ 的基底,則 $\alpha\omega_1, \cdots, \alpha\omega_n$ 構成 $[\alpha]$ 的基底,由定理 2 可知

$$N([\alpha])=\left|\sqrt{\frac{\Delta([\alpha])}{\Delta}}\right|=\left|\begin{vmatrix}\alpha^{(1)}\omega_1^{(1)}, \cdots, \alpha^{(1)}\omega_n^{(1)}\\ \cdots\cdots\cdots\cdots\\ \alpha^{(n)}\omega_1^{(n)}, \cdots, \alpha^{(n)}\omega_n^{(n)}\end{vmatrix}\Big/\begin{vmatrix}\omega_1^{(1)}, \cdots, \omega_n^{(1)}\\ \cdots\cdots\cdots\\ \omega_1^{(n)}, \cdots, \omega_n^{(n)}\end{vmatrix}\right|=$$

$$=|\alpha^{(1)}\cdots\alpha^{(n)}|=|N(\alpha)|.$$

故定理 3 成立.

定理 4. $N(\mathfrak{AB}) = N(\mathfrak{A})N(\mathfrak{B})$.

證: 因 $\mathfrak{A}$ 包有 $\mathfrak{AB}$, 所以由定理 14.9.4 可知將 $\mathfrak{A}$ 中元素依 mod $\mathfrak{AB}$ 分類,其類數等於

$$\frac{N(\mathfrak{AB})}{N(\mathfrak{A})}.$$

若能證明這個類數也等於 $N(\mathfrak{B})$,則定理明矣.

命 $\beta_1, \cdots, \beta_{N(\mathfrak{B})}$ 代表 mod $\mathfrak{B}$ 的剩餘類, 而由 §7 習題 1, 可知必有整數 $\alpha \in \mathfrak{A}$, 適合

$$([\alpha], \mathfrak{AB}) = \mathfrak{A}. \tag{2}$$

易見 $\alpha\beta_1, \cdots, \alpha\beta_{N(\mathfrak{B})}$ 均在 $\mathfrak{A}$ 中,且若 $j \neq k$ $(1 \leqslant j, k \leqslant n)$, 恆有

$$\alpha\beta_j \not\equiv \alpha\beta_k \pmod{\mathfrak{AB}}.$$

又由 (2) 式,可知對於 $\mathfrak{A}$ 中任何元素 γ, 必有整數 η, δ 使

$$\gamma = \eta\alpha + \delta, \quad \delta \in \mathfrak{AB}.$$

又對整數 η, 必有整數 β 及自然數 j $(1 \leqslant j \leqslant N(\mathfrak{B}))$,使

$$\eta = \beta_j + \beta,$$

於是得到

$$\gamma = \alpha\beta_j + \alpha\beta + \delta \equiv$$
$$\equiv \alpha\beta_j \pmod{\mathfrak{AB}}.$$

此卽 $\mathfrak{A}$ 中任一元素必與 $\alpha\beta_1, \cdots, \alpha\beta_{N(\mathfrak{B})}$ 中之一模 $\mathfrak{AB}$ 同餘,且僅與其中之一同餘. 因此若將 $\mathfrak{A}$ 中元素依 mod $\mathfrak{AB}$ 進行分類,其類數也等於 $N(\mathfrak{B})$, 於是定理得證.

定理 5. 若 $\mathfrak{P}$ 爲一素理想數, α 爲任何不能被 $\mathfrak{P}$ 整除的整數,則

$$\alpha^{N(\mathfrak{P})-1} \equiv 1 \pmod{\mathfrak{P}}.$$

證: 命 $0, \pi_1, \pi_2, \cdots, \pi_{N(\mathfrak{P})-1}$ 代表模 $\mathfrak{P}$ 的剩餘類, 則因 $\mathfrak{P} \nmid \alpha$, 所以 $0, \alpha\pi_1, \alpha\pi_2, \cdots, \alpha\pi_{N(\mathfrak{P})-1}$ 也代表模 $\mathfrak{P}$ 的剩餘類;因此

$$\alpha^{N(\mathfrak{P})-1}\pi_1\pi_2\cdots\pi_{N(\mathfrak{P})-1} \equiv \pi_1\pi_2\cdots\pi_{N(\mathfrak{P})-1} \pmod{\mathfrak{P}},$$

卽得定理.

§ 10. 素理想數.

定理 1. 凡素理想數 $\mathfrak{P}$ 必整除一有理素數 p, 且 p 爲 $\mathfrak{P}$ 中最小的有理

正整數,故是唯一的.

證: 由定理 7.1, 知必有有理整數 a 使 $\mathfrak{P}|[a]$, 分解 $a=\Pi p$, 故必有一 p 使 $\mathfrak{P}|[p]$,即 $\mathfrak{P}|p$.

假如有有理正整數 $b, b<p$, 且 $\mathfrak{P}|b$, 則 b 在 $\mathfrak{P}$ 中,故 $(p,b)=1$ 也在 $\mathfrak{P}$ 中,於是 $\mathfrak{P}=[1]$, 此乃不可能之事,故 p 是 $\mathfrak{P}$ 中最小的有理正整數.

將 $[p]$ 分解爲素理想數的乘積如

$$[p]=\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_t,$$

再於二邊取距得到

$$p^n=N([p])=N(\mathfrak{P}_1)N(\mathfrak{P}_2)\cdots N(\mathfrak{P}_t).$$

因此可知: 任一素理想數之距,必爲一素數之乘方. 若 $N(\mathfrak{P})=p^f$, f 稱爲 $\mathfrak{P}$ 之次數.

關於 $[p]$ 之分解有次之重要定理:

定理 2. $\mathfrak{P}^2|p$ 的必要且充分的條件爲 $p|\Delta$.

此定理稱爲 Dedekind 判別式定理,在本書中不預備給予證明.

今往考慮在二次域 $R(\sqrt{D})$ 中 $[p]$ 之分解,顯然祇有下列三種可能:

1) $[p]=\mathfrak{P}$;

2) $[p]=\mathfrak{P}\mathfrak{Q}$, $\mathfrak{P}\neq\mathfrak{Q}$, $N(\mathfrak{P})=N(\mathfrak{Q})=p$;

3) $[p]=\mathfrak{P}^2$, $N(\mathfrak{P})=p$.

關於 $[p]$ 在二次域中分解的情形,有次之定理:

定理 3. 1),2),3) 的成立當且僅當

$$\left(\frac{\Delta}{p}\right)=-1,+1,0,$$

此處 Δ 爲 $R(\sqrt{D})$ 的基數,$\left(\frac{\Delta}{p}\right)$ 爲 Kronecker 符號.

證: 若 $\mathfrak{P}$ 爲 $[p]$ 的素因子,而 $N(\mathfrak{P})=p$, 則此時

$$[p]=\mathfrak{P}\mathfrak{Q} \quad 或 \quad [p]=\mathfrak{P}^2.$$

命 cm, $c(n+\omega)$ 爲理想數的標準基底,則

$$N(\mathfrak{P})=c^2m=p,$$

故 $c=1$, $m=p$. 又因

$$\Delta \equiv \begin{cases} (2n+1)^2 \pmod{4p}, & \text{當} \quad D \equiv 1 \pmod 4; \\ (2n)^2 \pmod{4p}, & \text{當} \quad D \equiv 2,3 \pmod 4. \end{cases}$$

所以得到 $\left(\frac{\Delta}{p}\right) = 1$ 或 0.

反之,若 $\left(\frac{\Delta}{p}\right) = 1$ 或 0, 先考慮 $p \neq 2$ 的情形。

1) 若 $\left(\frac{\Delta}{p}\right) = 1$, 則有 a, $p \nmid a$, 使

$$\Delta \equiv a^2 \pmod p.$$

又因 $p \neq 2$, 所以 $(p, 2a) = 1$, 於是

$$[p, a+\sqrt{\Delta}]\cdot[p, a-\sqrt{\Delta}] = [p]\cdot\left[p, a+\sqrt{\Delta}, a-\sqrt{\Delta}, \frac{a^2-\Delta}{p}\right] =$$

$$= [p]\cdot[p, a+\sqrt{\Delta}, 2a, \frac{a^2-\Delta}{p}, 1] = [p].$$

又

$$[p, a+\sqrt{\Delta}] \neq [p, a-\sqrt{\Delta}],$$

蓋若不然,將有 $[p, a+\sqrt{\Delta}] = [p, a-\sqrt{\Delta}] = [p, a+\sqrt{\Delta}, 2a] = [1]$, 而此乃不可能之事,又 $[p, a+\sqrt{\Delta}]$ 及 $[p, a-\sqrt{\Delta}]$ 均非 $\mathfrak{O}$. 故當 $p \neq 2$, 而 $\left(\frac{\Delta}{p}\right) = 1$ 時, $[p]$ 爲二個不同的素理想數的乘積.

2) 若 $\left(\frac{\Delta}{p}\right) = 0$, 則 $p \mid \Delta$, 於是

$$[p, \sqrt{\Delta}]^2 = [p, \sqrt{\Delta}]\cdot[p, \sqrt{\Delta}] = [p]\cdot\left[p, \sqrt{\Delta}, \frac{\Delta}{p}\right],$$

但 $\Delta = D$ 或 $4D$, 今 $p \neq 2$, 而 D 又爲無平方因子數,所以 $\left(p, \frac{\Delta}{p}\right) = 1$, 故

$$[p] = [p, \sqrt{\Delta}]^2,$$

亦卽若 $p \neq 2$, 而 $\left(\frac{\Delta}{p}\right) = 0$, 則 $[p]$ 爲一素理想數的平方.

再考慮 $p = 2$ 的情形,因 $\left(\frac{\Delta}{2}\right) \neq -1$, 故必須 $D \equiv 2, 3 \pmod 4$ 或 $D \equiv 1 \pmod 8$. 與前面一樣,可證:

3) 當 $D \equiv 2 \pmod 4$ 時, $\left(\frac{\Delta}{2}\right) = 0$, 而 $[2] = [2, \sqrt{D}]^2$;

4) 當 $D \equiv 3 \pmod 4$ 時, 仍有 $\left(\frac{\Delta}{2}\right) = 0$, 而 $[2] = [2, 1+\sqrt{D}]^2$;

5) 當 $D \equiv 1 \pmod 8$ 時, $\left(\frac{\Delta}{2}\right) = 1$, 此時

$$[2]=\left[2,\frac{1+\sqrt{D}}{2}\right]\cdot\left[2,\frac{1-\sqrt{D}}{2}\right],$$

而 $\left[2,\frac{1+\sqrt{D}}{2}\right]\neq\left[2,\frac{1-\sqrt{D}}{2}\right]$, 故此時 [2] 分解爲二個不同的素理想數的乘積.

總結以上結果,卽得定理.

由定理 3, 可以看到 Dedekind 判別式定理在二次域中已成立. 今再具體的舉一三次域爲例.

命 α 爲

$$f(x)=x^3-x^2-2x-8=0$$

的根,在 §4 中已知 $R(\alpha)$ 爲一三次域,其基數爲 503, 且

$$1,\alpha,\beta=\frac{4}{\alpha}$$

爲他的一組整底,而 β 爲

$$g(y)=y^3+y^2+2y-8=0$$

的根.

今考慮 [503] 在 $R(\alpha)$ 上之分解. 以 $\mathfrak{P},\mathfrak{Q},\mathfrak{R}$ 代表 $R(\alpha)$ 上的素理想數,則 [503] 之分解必爲下列五種情形之一:

1) $[503]=\mathfrak{P}\mathfrak{Q}\mathfrak{R}$; $\mathfrak{P},\mathfrak{Q},\mathfrak{R}$ 各不相同,而 $N(\mathfrak{P})=N(\mathfrak{Q})=N(\mathfrak{R})=503$;

2) $[503]=\mathfrak{P}^2\mathfrak{Q}$; $\mathfrak{P}\neq\mathfrak{Q}$, 而 $N(\mathfrak{P})=N(\mathfrak{Q})=503$;

3) $[503]=\mathfrak{P}^3$; $N(\mathfrak{P})=503$;

4) $[503]=\mathfrak{P}\mathfrak{Q}$; $N(\mathfrak{P})=503$, $N(\mathfrak{Q})=503^2$;

5) $[503]=\mathfrak{P}$; $N(\mathfrak{P})=503^3$.

對於前四種情形,[503] 都有距爲 503 的素因子 $\mathfrak{P}$, 因此先考慮這種情形. 命

$$a_0,\ b_0+b_1\alpha,\ c_0+c_1\alpha+c_2\beta$$

爲 $\mathfrak{P}$ 之一組標準基底,則 $b_0<a_0$, $c_0<a_0$, $c_1<b_1$; 又因 $a_0\alpha, a_0\beta$ 均在 $\mathfrak{P}$ 中,所以又有 $b_1\leqslant a_0$, $c_2\leqslant a_0$, 於是由

$$N(\mathfrak{P})=a_0b_1c_2=503,$$

可得 $a_0=503$, $b_1=1$, $c_2=1$, $c_1=0$. 故 $\mathfrak{P}$ 必爲如下形式

$$\mathfrak{P}=[503,\ a+\alpha,\ b+\beta],$$

且 503, $a+\alpha$, $b+\beta$ 卽爲 $\mathfrak{P}$ 的標準基底.

因 $a+\alpha$, $b+\beta$ 均在 $\mathfrak{P}$ 中,而 $N(\mathfrak{P})=503$, 故有

$$N(a+\alpha)\equiv 0 \pmod{503};$$

$$N(b+\beta)\equiv 0 \pmod{503},$$

但 $a+\alpha$, $b+\beta$ 各爲 $f(x-a)=0$, 及 $g(y-b)=0$ 的根,所以

$$N(a+\alpha)=|f(-a)|,\quad N(b+\beta)=|g(-b)|,$$

故 a, b 適合三次同餘式

$$a^3+a^2-2a+8\equiv 0 \pmod{503};$$

$$b^3-b^2+2b+8\equiv 0 \pmod{503}.$$

由此解得

$$a\equiv 149,\ 149,\ 204 \pmod{503};$$

$$b\equiv 395,\ 395,\ 217 \pmod{503}.$$

所以 $\mathfrak{P}$ 必爲下列四者之一:

$$[503,\ 149+\alpha,\ 395+\beta];$$

$$[503,\ 204+\alpha,\ 217+\beta];$$

$$[503,\ 149+\alpha,\ 217+\beta];$$

$$[503,\ 204+\alpha,\ 395+\beta].$$

但 $\mathfrak{P}\neq[503,\ 149+\alpha,\ 217+\beta]$, 蓋若不然,則

$$\alpha(217+\beta)-217(149+\alpha)+65(503)=$$

$$=4-217\cdot 149+65\cdot 503=366$$

在 $\mathfrak{P}$ 中, 於是因 $(366, 503)=1$, 而得 $\mathfrak{P}=\mathfrak{O}$. 同樣 $\mathfrak{P}\neq[503,\ 204+\alpha,\ 395+\beta]$. 但因

$$(149+\alpha)\,\alpha=-46(503)+150(149+\alpha)+2(395+\beta),$$

$$(149+\alpha)\,\beta=-117(503)+149(395+\beta),$$

$$(395+\beta)\,\alpha=-117(503)+395(149+\alpha),$$

$$(395+\beta)\,\beta=-310(503)+2(149+\alpha)+394(395+\beta),$$

所以 $503, 149+\alpha$, $395+\beta$ 確爲素理想數 $[503, 149+\alpha,\ 395+\beta]$ 的標準基底;同樣, 503, $204+\alpha$, $217+\beta$ 確爲素理想數 $[503,\ 204+\alpha,\ 217+\beta]$ 的標準基底. 今

$$[503,\ 149+\alpha,\ 395+\beta] \mid [503],$$
$$[503,\ 204+\alpha,\ 217+\beta] \mid [503],$$

且

$$[503,\ 149+\alpha,\ 395+\beta] \neq [503,\ 204+\alpha,\ 217+\beta],$$

故在 [503] 之五種可能的分解中,祗有 2) 爲可能. 又由計算可得

$$[503] = [503,\ 149+\alpha,\ 395+\beta]^2 \cdot [503,\ 204+\alpha,\ 217+\beta].$$

習題. 設 $\vartheta = \sqrt[3]{pq^2}$, $\bar{\vartheta} = \sqrt[3]{p^2q}$,其中 p, q 爲有理素數,且滿足下述條件:

$$p \equiv 1 \pmod 3;\ q \neq 2,3;\ pq^2 \not\equiv 1 \pmod 9;\ q^{\frac{p-1}{3}} \not\equiv 1 \pmod p.$$

求證:

1) $R(\vartheta) = R(\bar{\vartheta})$ 爲一三次域;

2) $1, \vartheta, \bar{\vartheta}$ 爲 $R(\vartheta)$ 的一組整底;

3) $R(\vartheta)$ 中沒有整數 ω 使

$$1,\ \omega,\ \omega^2$$

成爲 $R(\vartheta)$ 的整底.

4) 試在 $R(\vartheta)$ 中分解下列理想數:

$$[2],\ [3],\ [p],\ [q].$$

§ 11. 單位數.

關於單位數有次之一般性的定理: 在域 $R(\vartheta)$ 之所有單位數中可以取出 $r = r_1 + r_2 - 1$ 個 $\varepsilon_1, \cdots, \varepsilon_r$, 使 $R(\vartheta)$ 中之任一單位數皆可以表爲

$$\rho \varepsilon_1^{l_1} \cdots \varepsilon_r^{l_r}, \quad l = 0, \pm 1, \pm 2, \cdots$$

之形式,此處 ρ 是某一單位根之在 $R(\vartheta)$ 中者.

爲簡單計,本書中僅研究二次域 $R(\sqrt{D})$. 命單位數爲 $x + y\omega$, 則

$$N(x + y\omega) = \pm 1,$$

所以祗要求出這個方程所有的有理整數解,就得到 $R(\sqrt{D})$ 中所有的單位數.

因爲

$$N(x+y\omega) = (x+y\omega)(x+y\omega') =$$
$$= \begin{cases} \left(x + \dfrac{y}{2}\right)^2 - \dfrac{y^2}{4} D, & \text{若}\ D \equiv 1 \pmod 4; \\ x^2 - y^2 D, & \text{若}\ D \equiv 2,3 \pmod 4), \end{cases}$$

當 $D<0$ 時,

$$(2x+y)^2-y^2D=4$$

及

$$x^2-y^2D=1$$

都祇能有有限個解,故當 $D<0$ 時, $R(\sqrt{D})$ 內祇有有限個單位數. 若以 w 表 $R(\sqrt{D})$ 內單位數之個數,則不難證明當 $\Delta=-3,-4$, 及 $\Delta\leqslant-7$ 時 $w=6,4,2$.

今往研究 $D>0$ 之情況,此時

$$(2x+y)^2-y^2D=\pm 4$$

及

$$x^2-y^2D=\pm 1$$

均爲第十章之 Pell 方程. 故在 $R(\sqrt{D})$ 中有一單位數 η 存在,使凡 $R(\sqrt{D})$ 中之單位數皆可表爲

$$\pm\eta^n,\quad n=0,\pm 1,\pm 2,\cdots$$

的形式. η 稱爲 $R(\sqrt{D})$ 的基本單位數.

習題. 試證若基本單位數 $\eta=X+Y\sqrt{D}$ 的係數爲有理整數,則 X,Y 爲

$$u^2-v^2D=N(\eta)$$

的最小正整數解. 若 X,Y 不是有理整數,則 $\eta^3=u+v\sqrt{D}$ 的係數 u,v 卽爲上式的最小正整數解.

§ 12. 理想數類.

定義 1. 對於二理想數 $\mathfrak{A}$ 及 $\mathfrak{B}$, 若有二主理想數 $[\alpha]$ 及 $[\beta]$ 使

$$[\alpha]\mathfrak{A}=[\beta]\mathfrak{B},$$

則此二理想數謂之屬於同一理想數類. 以 $\mathfrak{A}\sim\mathfrak{B}$ 記之.

易見有以下諸性質:

1) $\mathfrak{A}\sim\mathfrak{A}$;

2) 若 $\mathfrak{A}\sim\mathfrak{B}$, 則 $\mathfrak{B}\sim\mathfrak{A}$;

3) 若 $\mathfrak{A}\sim\mathfrak{B}$, $\mathfrak{B}\sim\mathfrak{C}$, 則 $\mathfrak{A}\sim\mathfrak{C}$;

4) 若 $\mathfrak{A}\sim\mathfrak{O}$, 則 $\mathfrak{A}$ 爲主理想數,且逆之亦然;

5) 若 $\mathfrak{A}\sim\mathfrak{B}$, $\mathfrak{C}\sim\mathfrak{D}$, 則 $\mathfrak{A}\mathfrak{C}\sim\mathfrak{B}\mathfrak{D}$;

6) 若 $\mathfrak{A}\mathfrak{C}\sim\mathfrak{B}\mathfrak{C}$, 則 $\mathfrak{A}\sim\mathfrak{B}$.

因此可將 $R(\vartheta)$ 上所有的理想數進行分類,稱爲理想數類.

定理 1. $R(\vartheta)$ 上的理想數類之個數有限.

證: 如能證明: 有一僅與 $R(\vartheta)$ 有關的正數 M 存在, 使每一類中有一理想數 $\mathfrak{B}$ 適合

$$N(\mathfrak{B})\leqslant M,$$

則定理已經證明,蓋因以一固定數爲距的理想數僅有有限個也.

命 $\mathfrak{C}$ 爲 $R(\vartheta)$ 上任何理想數,由前已知必有理想數 $\mathfrak{A}$, 使

$$\mathfrak{A}\,\mathfrak{C}\sim\mathfrak{O},$$

若能選擇一 $\mathfrak{B}$ 使

$$\mathfrak{A}\,\mathfrak{B}\sim\mathfrak{O},$$

且

$$N(\mathfrak{B})\leqslant M,$$

則定理已經證明. 蓋因 $\mathfrak{A}\mathfrak{B}\sim\mathfrak{A}\mathfrak{C}$, 可知 $\mathfrak{B}\sim\mathfrak{C}$ 也.

命 $\omega_1,\cdots,\omega_n$ 爲 $R(\vartheta)$ 之一組整底,命

$$M=\prod_{s=1}^{n}(|\omega_1^{(s)}|+\cdots+|\omega_n^{(s)}|),$$

今往證此 M 卽爲所求.

取自然數 k 適合於

$$k^n\leqslant N(\mathfrak{A})<(k+1)^n,$$

在 $(k+1)^n$ 個整數

$$x_1\,\omega_1+\cdots+x_n\,\omega_n\quad(x_m=0,1,\cdots,k)$$

中至少有兩個對模 $\mathfrak{A}$ 同餘, 命爲

$$y_1\,\omega_1+\cdots+y_n\,\omega_n\equiv z_1\,\omega_1+\cdots+z_n\,\omega_n\pmod{\mathfrak{A}},$$

此處 $0\leqslant y_m\leqslant k$, $0\leqslant z_m\leqslant k$, 卽得一不等於 0 的整數

$$\alpha=(y_1-z_1)\,\omega_1+\cdots+(y_n-z_n)\,\omega_n$$

在 $\mathfrak{A}$ 之中,因爲 $|y_m-z_m|\leqslant k$, 故得

$$|N(\alpha)|=\left|\prod_{s=1}^{n}\sum_{m=1}^{n}(y_m-z_m)\,\omega_m^{(s)}\right|\leqslant\prod_{s=1}^{n}\sum_{m=1}^{n}k\,|\omega_m^{(s)}|=k^nM\leqslant$$

$$\leqslant M\cdot N(\mathfrak{A}).$$

因 α 在 $\mathfrak{A}$ 中,故 $\mathfrak{A}|[\alpha]$, 令 $[\alpha]=\mathfrak{A}\mathfrak{B}$, 則

$$N(\mathfrak{A})\,N(\mathfrak{B})=|N(\alpha)|\leqslant M\cdot N(\mathfrak{A}),$$

亦卽

$$N(\mathfrak{B})\leqslant M,$$

定理得證.

定理 2. 命 h 爲 $R(\vartheta)$ 上理想數類的類數,則任一理想數 $\mathfrak{A}$ 皆適合於

$$\mathfrak{A}^h\sim\mathfrak{O},$$

$\mathfrak{A}^h$ 表示 h 個 $\mathfrak{A}$ 的連乘積.

證: 命

$$\mathfrak{A}_1,\cdots,\mathfrak{A}_h$$

代表不同的理想數類,則

$$\mathfrak{A}\,\mathfrak{A}_1,\cdots,\mathfrak{A}\,\mathfrak{A}_h$$

亦然. 故必

$$\mathfrak{A}_1\cdots\mathfrak{A}_h\sim(\mathfrak{A}\,\mathfrak{A}_1)\cdots(\mathfrak{A}\,\mathfrak{A}_h),$$

亦卽

$$\mathfrak{A}^h\sim\mathfrak{O}.$$

§ 13. 二次域與二次型.

以 Δ 表示二次域 $R(\sqrt{D})$ 的基數. 今往建立 $R(\sqrt{D})$ 上理想數類與以 Δ 爲判別式的二次型之類之間的關係.

命 $\mathfrak{A}$ 爲 $R(\sqrt{D})$ 上之一理想數,並設 α_1,α_2 爲 $\mathfrak{A}$ 的一組基底,且適合

$$\alpha_1\,\alpha_2'-\alpha_1'\,\alpha_2=N(\mathfrak{A})\sqrt{\Delta}\,, \tag{1}$$

此處 α_1',α_2' 表示 α_1,α_2 的共軛數.

對應於 $\mathfrak{A}$ 作二次型

$$F(x,y)=\frac{N(\alpha_1\,x+\alpha_2\,y)}{N(\mathfrak{A})}=\frac{(\alpha_1\,x+\alpha_2\,y)\,(\alpha_1'\,x+\alpha_2'\,y)}{N(\mathfrak{A})}=$$
$$=ax^2+bxy+cy^2,$$

因 α_1,α_2, $\alpha_1+\alpha_2$ 均在 $\mathfrak{A}$ 中,而 $a=\dfrac{N(\alpha_1)}{N(\mathfrak{A})}$, $b=\dfrac{N(\alpha_1+\alpha_2)-N(\alpha_1)-N(\alpha_2)}{N(\mathfrak{A})}$, $c=\dfrac{N(\alpha_2)}{N(\mathfrak{A})}$, 故 a,b,c 均爲有理整數. 又 $F(x,y)$ 之判别式爲

$$b^2-4ac=\frac{(\alpha_1\,\alpha_2'-\alpha_1'\,\alpha_2)^2}{N(\mathfrak{A})^2}=\Delta,$$

故 $F(x,y)$ 爲一判別式爲 Δ，且有有理整係數的二次型．稱 $F(x,y)$ 爲屬於 $\mathfrak{A}$ 的二次型．

當 $\Delta<0$ 時，$R(\sqrt{D})$ 爲虛域，故必 $a>0$，而 $F(x,y)$ 爲定正。

又由定義，不難看到：若取 α_1,α_2 經過 $\mathfrak{A}$ 的所有適合 (1) 式的基底，就可得到所有與 F 相似的二次型．

定理 1. 對於任一以 Δ 爲判別式的且有有理整係數的不定型或正定型

$$F(x,y)=ax^2+bxy+cy^2,$$

必有理想數 $\mathfrak{A}$，及其基底 α_1,α_2，使 F 屬於 $\mathfrak{A}$．

證：先證 $a,\frac{b-\sqrt{\Delta}}{2}$ 爲理想數

$$\mathfrak{M}=\left[a,\frac{b-\sqrt{\Delta}}{2}\right]$$

的基底．因 $\frac{b-\sqrt{\Delta}}{2}$ 適合 $x(b-x)=ac$，故 $\frac{b-\sqrt{\Delta}}{2}$ 爲一整數．又因

$$\omega=\frac{s(\omega)+\sqrt{\Delta}}{2}$$

恆成立，且

$$a\omega=\frac{s(\omega)+b-(b-\sqrt{\Delta})}{2}a=\frac{s(\omega)+b}{2}a-a\frac{b-\sqrt{\Delta}}{2},$$

$$\frac{b-\sqrt{\Delta}}{2}\omega=\frac{b-\sqrt{\Delta}}{2}\cdot\frac{s(\omega)-b+b+\sqrt{\Delta}}{2}=\frac{b^2-\Delta}{4a}a+\frac{s(\omega)-b}{2}\cdot\frac{b-\sqrt{\Delta}}{2},$$

而 $\frac{s(\omega)\pm b}{2},\frac{b^2-\Delta}{4a}$ 皆爲有理整數，故 $a,\frac{b-\sqrt{\Delta}}{2}$ 確爲 $\mathfrak{M}$ 的基底．

若 $a>0$，取 $\mathfrak{A}=\mathfrak{M}$，$\alpha_1=a$，$\alpha_2=\frac{b-\sqrt{\Delta}}{2}$，因 $N(\mathfrak{M})=a$，由此作出二次型

$$\frac{\left(ax+\frac{1}{2}(b-\sqrt{\Delta})y\right)\left(ax+\frac{1}{2}(b+\sqrt{\Delta})y\right)}{a}=ax^2+bxy+cy^2,$$

故 $\mathfrak{M}=\left[a,\frac{b-\sqrt{\Delta}}{2}\right]$ 即爲所求．

若 $a<0$，因爲我們不討論定負型，故 $\Delta>0$，取

$$\mathfrak{A}=\sqrt{\Delta}\,\mathfrak{M}$$

及 $\alpha_1=a\sqrt{\Delta}$，$\alpha_2=\frac{b-\sqrt{\Delta}}{2}\sqrt{\Delta}$，易見 α_1,α_2 即爲 $\mathfrak{A}$ 之基底，且適合 (1)

式，又 $N(\mathfrak{A}) = -a\Delta$. 由此作出二次型，得

$$\frac{-\Delta\left(ax+\frac{1}{2}(b-\sqrt{\Delta})\,y\right)\left(ax+\frac{1}{2}(b+\sqrt{\Delta})\,y\right)}{-a\Delta} = ax^2+bxy+cy^2,$$

定理得證.

在上面已經看到：若 F 屬於 $\mathfrak{A}$，則所有與 F 相似的二次型亦均屬於 $\mathfrak{A}$. 但是，對於一個二次型 F，也可以有不同的理想數 $\mathfrak{A}, \mathfrak{B}$，使 F 屬於 $\mathfrak{A}$，亦屬於 $\mathfrak{B}$. 下面將給出這種 $\mathfrak{A}, \mathfrak{B}$ 間之關係.

定義 1. 若二理想數 $\mathfrak{A}$ 與 $\mathfrak{B}$ 之間有次之關係，卽有整數 α 與 β 使

$$[\alpha]\,\mathfrak{A} = [\beta]\,\mathfrak{B} \quad 而 \quad N(\alpha\beta) > 0$$

成立，則謂之狹義相似，以 $\mathfrak{A} \approx \mathfrak{B}$ 表之.

顯然，狹義相似乃相似之一種特殊情形.

定理 2. 相似型屬於狹義相似之理想數，且逆之亦眞.

證：命 α_1, α_2 及 β_1, β_2 各爲 $\mathfrak{A}$ 與 $\mathfrak{B}$ 之底，且都適合 (1) 式，又命

$$F(x,y) = \frac{N(\alpha_1 x+\alpha_2 y)}{N(\mathfrak{A})}; \quad G(x,y) = \frac{N(\beta_1 x+\beta_2 y)}{N(\mathfrak{B})}.$$

若 $F \sim G$，則有一組有理整數 a, b, c, d 使 $ad-bc=1$，且使

$$F(ax+by, cx+dy) = G(x,y),$$

亦卽

$$\frac{N((a\alpha_1+c\alpha_2)\,x+(b\alpha_1+d\alpha_2)\,y)}{N(\mathfrak{A})} = \frac{N(\beta_1 x+\beta_2 y)}{N(\mathfrak{B})}. \tag{3}$$

因爲 $-\frac{\beta_2}{\beta_1}, -\frac{\beta_2'}{\beta_1'}$ 爲 $G(x,1)=0$ 的二根，而 $-\frac{b\alpha_1+d\alpha_2}{a\alpha_1+c\alpha_2}$ 也能使 $G(x,1)=0$，故有

$$\frac{b\alpha_1+d\alpha_2}{a\alpha_1+c\alpha_2} = \frac{\beta_2}{\beta_1} \quad 或 \quad \frac{\beta_2'}{\beta_1'},$$

卽有代數數 λ 使

$$a\alpha_1+c\alpha_2 = \lambda\beta_1 \quad 或 \quad \lambda\beta_1',$$

$$b\alpha_1+d\alpha_2 = \lambda\beta_2 \quad 或 \quad \lambda\beta_2'.$$

以此代入 (3) 得

$$N(\lambda) = \lambda\lambda' = \frac{N(\mathfrak{A})}{N(\mathfrak{B})} > 0.$$

今謂在這二種情況中，祇能

$$a\alpha_1 + c\alpha_2 = \lambda\beta_1, \quad b\alpha_1 + d\alpha_2 = \lambda\beta_2 \tag{4}$$

成立，蓋若不然，將有

$$(ad - bc)(\alpha_1\alpha_2' - \alpha_1'\alpha_2) = -\lambda\lambda'(\beta_1\beta_2' - \beta_2\beta_1'),$$

亦卽

$$N(\mathfrak{A})\sqrt{\Delta} = -N(\lambda)N(\mathfrak{B})\sqrt{\Delta},$$

此與已經得到的 $N(\lambda) > 0$ 相矛盾，故祗能 (4) 式成立.

由定理 1.4 可知能將 λ 表爲二個整數之商如 $\frac{\beta}{\alpha}$，於是

$$a(\alpha\alpha_1) + c(\alpha\alpha_2) = \beta\beta_1, \quad b(\alpha\alpha_1) + d(\alpha\alpha_2) = \beta\beta_2, \tag{5}$$

因 $\alpha\alpha_1, \alpha\alpha_2$ 與 $\beta\beta_1, \beta\beta_2$ 爲理想數 $[\alpha]\mathfrak{A}$ 與 $[\beta]\mathfrak{B}$ 的基底，又因 $ad - bc = 1$，所以 $\beta\beta_1, \beta\beta_2$ 也是 $[\alpha]\mathfrak{A}$ 的基底，於是得到

$$[\alpha]\mathfrak{A} = [\beta]\mathfrak{B}.$$

又 $N\left(\frac{\beta}{\alpha}\right) = N(\lambda) > 0$，所以 $N(\alpha\beta) > 0$，因此 $\mathfrak{A}, \mathfrak{B}$ 爲狹義相似.

反之若 $\mathfrak{A}, \mathfrak{B}$ 爲狹義相似，卽有整數 α, β 使

$$[\alpha]\mathfrak{A} = [\beta]\mathfrak{B}, \quad N(\alpha\beta) > 0.$$

命 α_1, α_2 與 β_1, β_2 爲 $\mathfrak{A}$ 與 $\mathfrak{B}$ 之基底，且適合 (1) 式，則 $\alpha\alpha_1, \alpha\alpha_2$ 與 $\beta\beta_1, \beta\beta_2$ 爲 $[\alpha]\mathfrak{A}$ 與 $[\beta]\mathfrak{B}$ 之基底. 所以有有理整數 a, b, c, d 適合 $|ad - bc| = 1$，使 (5) 式成立. 又因 $N(\alpha\beta) > 0$；而 α_1, α_2 與 β_1, β_2 適合 (1) 式，故 $ad - bc = 1$. 又因

$$N(\alpha)N(\mathfrak{A}) = N(\beta)N(\mathfrak{B}),$$

所以 (3) 式成立，亦卽 $F \sim G$，定理得證.

命 h_0 表示理想數類（非狹義的）的類數，而以 h 表示狹義相似意義下的理想數類的類數，假設他們所在域的基數爲 Δ，則 h 亦卽以 Δ 爲判別式的二次型類的類數.

因若 $\mathfrak{A} \sim \mathfrak{B}$，則必須 $\mathfrak{A} \approx \mathfrak{B}$ 或者 $\mathfrak{A} \approx [\sqrt{\Delta}]\mathfrak{B}$，所以 $h \leqslant 2h_0$. 事實上，若 $\mathfrak{A} \sim \mathfrak{B}$，則有整數 α, β 使

$$[\alpha]\mathfrak{A} = [\beta]\mathfrak{B}.$$

i) 若 $\Delta < 0$，則必 $N(\alpha\beta) > 0$，故此時 $\mathfrak{A} \approx \mathfrak{B}$，所以 $h_0 = h$.

ii) 若 $\Delta > 0$，而基本單位數 η 適合 $N(\eta) = -1$，則因

$$[\alpha]\,\mathfrak{A}=[\beta]\,\mathfrak{B}=[\eta\,\beta]\,\mathfrak{B},$$

而 $N(\alpha\beta)$ 與 $N(\alpha\beta\eta)$ 必有一爲正,故此時也有 $\mathfrak{A}\approx\mathfrak{B}$, 而 $h_0=h$.

iii) 若 $\Delta>0$, 而基本單位數 η 適合 $N(\eta)=1$, 則若 $\mathfrak{A}\approx\mathfrak{B}$, 就決不能有 $\mathfrak{A}\approx\mathfrak{B}\,[\sqrt{\Delta}]$. 故此時 $h_0=\frac{1}{2}h$.

故得

$$h_0=\begin{cases} h, & \text{若 } \Delta<0, \text{ 或當 } \Delta>0,\ N(\eta)=-1;\\ \frac{1}{2}h, & \text{若 } \Delta>0, \text{ 而 } N(\eta)=+1.\end{cases}$$

又在定理 11.4.4 中換 d 爲 D, 而類似的定義 ε, 則

$$\varepsilon=\begin{cases}\eta^2, & \text{若 } \Delta>0, \text{ 而 } N(\eta)=-1;\\ \eta, & \text{若 } \Delta>0, \text{ 而 } N(\eta)=1.\end{cases}$$

再由第十二章中所得關於類數的結果,可得:

定理 3. 命 h_0 表理想數類的個數,則

$$h_0=\frac{W}{2\left(2-\left(\frac{\Delta}{2}\right)\right)}\sum_{s=1}^{\left[\frac{1}{2}|\Delta|\right]}\left(\frac{\Delta}{s}\right),\qquad \text{若 } \Delta<0,$$

$$\eta^{h_0}=\prod_{s=1}^{\left[\frac{1}{2}(\Delta-1)\right]}\left(\sin\frac{s\pi}{\Delta}\right)^{-\left(\frac{\Delta}{s}\right)},\qquad \text{若 } \Delta>0.$$

例 1. 在 $R(i)$ 中, $\Delta=-4$, $W=4$, 故

$$h_0=\frac{4}{2(2-0)}\sum_{s=1}^{2}\left(\frac{-4}{s}\right)=1.$$

例 2. 在 $R(\sqrt{-3})$ 中, $\Delta=-3$, $W=6$, 故

$$h_0=\frac{6}{2(2-(-1))}\sum_{s=1}^{1}\left(\frac{-3}{s}\right)=1.$$

例 3. 在 $R(\sqrt{-5})$ 中, $\Delta=-20$, $W=2$, 故

$$h_0=\frac{2}{2(2-0)}\sum_{s=1}^{10}\left(\frac{-20}{s}\right)=$$

$$=\frac{1}{2}\left(\left(\frac{-20}{1}\right)+\left(\frac{-20}{3}\right)+\left(\frac{-20}{7}\right)+\left(\frac{-20}{9}\right)\right)=2.$$

例 4. 在 $R(\sqrt{-19})$ 中, $\Delta=-19$, $W=2$, 則

$$h_0=\frac{2}{2(2-(-1))}\sum_{s=1}^{9}\left(\frac{-19}{s}\right)=$$

$$=\frac{1}{3}\left\{\left(\frac{-19}{1}\right)+\left(\frac{-19}{2}\right)+\left(\frac{-19}{3}\right)+\left(\frac{-19}{4}\right)+\left(\frac{-19}{5}\right)+\right.$$

$$\left.+\left(\frac{-19}{6}\right)+\left(\frac{-19}{7}\right)+\left(\frac{-19}{8}\right)+\left(\frac{-19}{9}\right)\right\}=1.$$

例 5. 在 $R(\sqrt{2})$ 中, $\Delta=8$, $\varepsilon=3+2\sqrt{2}$, 因 $\eta=1+\sqrt{2}$ 之距爲 -1, 且其平方爲 ε, 故爲域之基本單位數. 又因

$$(1+\sqrt{2})^{h_0}=\prod_{s=1}^{3}\left(\sin\frac{\pi s}{8}\right)^{-\left(\frac{8}{s}\right)}=\sin\frac{3\pi}{8}\Big/\sin\frac{\pi}{8}=(1+\sqrt{2}),$$

故 $h_0=1$.

§14. 族.

固定一個二次域 $R(\sqrt{D})$, 其基數爲 Δ, 並假定本節中所述及的理想數類都是在狹義相似意義下的理想數類.

定義 1. 若二次型 $F(x,y)$ 屬於理想數 $\mathfrak{A}$, 則稱 $F(x,y)$ 的特徵系爲理想數 $\mathfrak{A}$ 的特徵系. 亦卽若命 $p_1,\cdots,p_s$ 爲 Δ 的奇素因子, 取 $\mathfrak{A}$ 中整數 α 之使 $\left(\frac{N(\alpha)}{N(\mathfrak{A})},2\Delta\right)=1$ 成立者, 稱

$$\left(\frac{N(\alpha)/N(\mathfrak{A})}{p_i}\right)\qquad(i=1,\cdots,s)$$

及

$$\delta(\alpha)=(-1)^{\frac{1}{2}\left[\frac{N(\alpha)}{N(\mathfrak{A})}-1\right]},\qquad 若\ D=\frac{\Delta}{4}\equiv 3\pmod 4;$$

$$\varepsilon(\alpha)=(-1)^{\frac{1}{8}\left[\left(\frac{N(\alpha)}{N(\mathfrak{A})}\right)^2-1\right]},\qquad 若\ \frac{\Delta}{4}\equiv 2\pmod 8;$$

$$\delta(\alpha)\,\varepsilon(\alpha),\qquad 若\ \frac{\Delta}{4}\equiv 6\pmod 8$$

爲理想數 $\mathfrak{A}$ 的特徵系.

因屬於同一類的理想數有相同的特徵系, 因此可以定義理想數類的特徵系.

定義 2. 二個具有相同特徵系的類稱爲屬於同一族, 於是在二次域 $R(\sqrt{D})$ 上的理想數類與以 Δ 爲判别式的原型類間就有一一對應的關係.

定理 1. 理想數 $\mathfrak{A}\mathfrak{B}$ 的特徵系中各值, 卽爲 $\mathfrak{A},\mathfrak{B}$ 的對應特徵值的乘積.

證: 因若 α 在 $\mathfrak{A}$ 中, β 在 $\mathfrak{B}$ 中,則 $\alpha\beta$ 在 $\mathfrak{A}\beta$ 中. 又

$$\frac{N(\alpha)}{N(\mathfrak{A})}\cdot\frac{N(\beta)}{N(\mathfrak{B})}=\frac{N(\alpha\beta)}{N(\mathfrak{A}\mathfrak{B})},$$

及

$$\frac{N(\alpha\beta)}{N(\mathfrak{A}\mathfrak{B})}-1\equiv\frac{N(\alpha)}{N(\mathfrak{A})}-1+\frac{N(\beta)}{N(\mathfrak{B})}-1 \pmod 4,$$

$$\left(\frac{N(\alpha\beta)}{N(\mathfrak{A}\mathfrak{B})}\right)^2-1\equiv\left(\frac{N(\alpha)}{N(\mathfrak{A})}\right)^2-1+\left(\frac{N(\beta)}{N(\mathfrak{B})}\right)^2-1 \pmod{16},$$

且若 $\left(\frac{N(\alpha)}{N(\mathfrak{A})},\ 2\Delta\right)=1,\left(\frac{N(\beta)}{N(\mathfrak{B})},\ 2\Delta\right)=1$, 則 $\left(\frac{N(\alpha\beta)}{N(\mathfrak{A}\mathfrak{B})},\ 2\Delta\right)=1$, 故得定理.

由定理立刻得到:

1) 二類乘積的特徵系即爲二類特徵系的乘積;

2) 若類 $\{\mathfrak{A}\}$ 與類 $\{\mathfrak{B}\}$ 在同一族中,類 $\{\mathfrak{A}_1\}$ 與類 $\{\mathfrak{B}_1\}$ 在同一族中,則類 $\{\mathfrak{A}\mathfrak{B}\}$ 與 $\{\mathfrak{A}_1\mathfrak{B}_1\}$ 也在同一族中.

定義 3. 稱單位理想數 $\mathfrak{O}$ 所屬之類爲主類,主類所屬之族爲主族. 又若 $\mathfrak{A}\mathfrak{B}=[a]$, a 爲一自然數,則稱類 $\{\mathfrak{B}\}$ 爲類 $\{\mathfrak{A}\}$ 之逆類.

由定理 7.1 可知任何理想數類的逆類一定存在. 又

$$\{\mathfrak{O}\}\{\mathfrak{A}\}=\{\mathfrak{A}\}.$$

因主類及主族中各類的各特徵值都是 1, 所以主族中任何二類的乘積還在主族中,主族中任何一類的逆類還在主族中.*

定理 2. 每一族中的類數相等.

證: 用 $\mathfrak{J}$ 表示主族,而用 $\mathfrak{J}\{\mathfrak{A}\}$ 表示 $\mathfrak{J}$ 中各類與 $\{\mathfrak{A}\}$ 的乘積類的集合. 若將所有的理想數類分爲若干集合:

$$\mathfrak{J},\ \mathfrak{J}\{\mathfrak{A}_2\},\ \mathfrak{J}\{\mathfrak{A}_3\},\cdots,\mathfrak{J}\{\mathfrak{A}_g\},\tag{1}$$

其中 $\{\mathfrak{A}_i\}$ 是任何類之不在 $\mathfrak{J},\mathfrak{J}\{\mathfrak{A}_2\},\cdots,\mathfrak{J}\{\mathfrak{A}_{i-1}\}$ 中者. 易見必無理想數類同時屬於 (1) 中二個不同的集合.

由定理 1, 可知 (1) 中任一集合內的各類都在同一族中. 又 (1) 中不同的集合屬於不同的族,所以 (1) 中每一集合即爲一族. 又因 $\mathfrak{J}\{\mathfrak{A}_i\}$ 中任何二類都不相同,故得定理.

---

*全體理想數類對類的乘積成一羣,主族中各類對此運算也成一羣.

習題 1. 當 $\Delta > 0$, 而基本單位數適合 $N(\eta) = +1$ 時, 試求理想數 $[\sqrt{\Delta}]$ 的特徵系.

習題 2. 若理想數 $\mathfrak{A}$ 的特徵系與 $\mathfrak{B}$ 或 $\mathfrak{B}[\sqrt{\Delta}]$ 的特徵系相同, 則稱 $\mathfrak{A}$ 與 $\mathfrak{B}$ 爲屬於同一族 (廣義的). 試證在這樣的定義之下, 若 $\mathfrak{A} \sim \mathfrak{B}$, 則 $\mathfrak{A}, \mathfrak{B}$ 必屬於同一族, 且每一族中所含的類數相同.

§ 15. 歐幾里得域與單域.

定 義 1. 若 $h_0 = 1$, 則該域稱爲單域.

顯然若域爲單域, 則其上之理想數都是主理想數, 故得:

定 理 1. 凡單域中整數之唯一分解定理成立.

有一種單域具有與有理數域很相似之性質, 稱之爲歐幾里得域.

定 義 2. 若對 $R(\sqrt{D})$ 中任意二個整數 $\xi, \eta (\eta \neq 0)$, 恆有二整數 κ 與 λ 存在, 使

$$\xi = \kappa\eta + \lambda, \quad |N(\lambda)| < |N(\eta)|, \tag{1}$$

則該域稱爲歐幾里得域, 並簡稱之爲歐氏域.

亦可定義如下:

定 義 3. 若對 $R(\sqrt{D})$ 中任意一數 δ, 必有一整數 κ 使

$$|N(\delta - \kappa)| < 1, \tag{2}$$

則 $R(\sqrt{D})$ 稱爲歐幾里得域.

定 理 2. 凡歐幾里得域必爲單域.

證: 若 $R(\sqrt{D})$ 爲歐幾里得域, 欲證其爲一單域, 僅須證明 $R(\sqrt{D})$ 上每一理想數均爲主理想數, 便已足够.

命 $\mathfrak{A}$ 爲 $R(\sqrt{D})$ 上任何一個理想數, 以 α_1, α_2 表示 $\mathfrak{A}$ 的一組基底, 不失普遍性我們可以假定

$$0 < |N(\alpha_1)| \leqslant |N(\alpha_2)|.$$

由 $R(\sqrt{D})$ 爲歐幾里得域之假定, 可知有整數 α_2' 及 β_2, 使

$$\alpha_2 = \alpha_2'\alpha_1 + \beta_2, \quad |N(\beta_2)| < |N(\alpha_1)|.$$

若 $\beta_2 \neq 0$, 則又有 α_1' 及 β_1 使

$$\alpha_1 = \alpha_1'\beta_2 + \beta_1, \quad |N(\beta_1)| < |N(\beta_2)|,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots.$$

因 $|N(\alpha_1)|$ 爲一有限的自然數, 故經有限次手續後, 必能得到整數 α 使

$$\mathfrak{A} = [\alpha_1, \alpha_2] = [\alpha],$$

定理得證。

定 理 3. 僅有五個二次虛歐幾里得域:

$$\Re(\sqrt{-1}), \Re(\sqrt{-2}), \Re(\sqrt{-3}), \Re(\sqrt{-7}), \Re(\sqrt{-11}).$$

證: 1) 若 $D \equiv 2, 3 \pmod 4$. 取 $\delta = r + s\sqrt{D}$, $\kappa = x + y\sqrt{D}$, 則 (2) 式變爲對任意一對有理數 r, s 有有理整數 x, y 使

$$|(r-x)^2 - D(s-y)^2| < 1. \tag{3}$$

若取 $r = s = \frac{1}{2}$,則由 (3) 可得

$$\frac{1}{4} + |D|\frac{1}{4} < 1, \quad 卽 \quad |D| < 3.$$

故若 $|D| \geqslant 3$, 則 $R(\sqrt{D})$ $(D < 0)$ 非歐幾里得域.

因對任何有理數 r,s 恆有有理整數 x, y 使

$$|r-x| \leqslant \frac{1}{2}, \quad |s-y| \leqslant \frac{1}{2},$$

故對 $D = -1, -2$,

$$|(r-x)^2 - D(s-y)^2| \leqslant \frac{1}{4} + |D|\frac{1}{4} < 1$$

恆成立,所以 $R(\sqrt{-1})$, $R(\sqrt{-2})$ 爲歐幾里得域.

2) 若 $D \equiv 1 \pmod 4$. 取

$$\delta = r + s\sqrt{D}, \quad \kappa = x + \frac{1}{2}y(1+\sqrt{D}),$$

故得

$$\left|\left(r - x - \frac{1}{2}y\right)^2 - D\left(s - \frac{1}{2}y\right)^2\right| < 1. \tag{4}$$

取 $r = s = \frac{1}{4}$,則得

$$\frac{1}{16} + \frac{1}{16}|D| < 1, \quad 卽 \quad |D| < 15.$$

故當 $D \equiv 1 \pmod 4$時,僅可能有三個歐幾里得域 $R(\sqrt{-3}), R(\sqrt{-7}), R(\sqrt{-11})$. 反之,因爲對任何有理數 r,s 總有有理整數 x,y 使

$$|2s-y| \leqslant \frac{1}{2}, \quad \left|r - x - \frac{1}{2}y\right| \leqslant \frac{1}{2},$$

於是當 $D = -3, -7, -11$ 時

$$\left|\left(r-x-\frac{1}{2}y\right)^2 - D\left(s-\frac{1}{2}y\right)^2\right| \leqslant \frac{1}{4} + |D|\frac{1}{16} \leqslant \frac{15}{16} < 1.$$

故此三域確爲歐幾里得域,定理得證.

前節已經算出 $R(\sqrt{-19})$ 之類數是 1, 由上定理可知其非歐幾里得域,是以有非歐幾里得域之單域存在.

由定理 12.15.4 可知僅有有限個虛域是單域. 問題在於究竟有幾個? 易於算出,若

$$D = -1, -2, -3, -7, -11, -19, -43, -67, -163,$$

則 $R(\sqrt{D})$ 是單域. 並有人證明至多還有一個,而假如存在的話,則必 $D < <-5\cdot 10^9$.

關於實歐氏域的問題,有次之定理:

定理 4. $R(\sqrt{D})$ 當且僅當

$$D = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$$

時爲實歐氏域.

其證明超出本書範圍,故略去.

附註: 關於實歐幾里得域的問題,我國數學家楊武之、柯召、閔嗣鶴及作者皆曾有貢獻. 此問題基本上是由 Davenport 最後解決的.

§ 16. 判斷 Mersenne 數是否素數之 Lucas 條件.

今先使定理 9.6 在二次域 $R(\sqrt{D})$ $(D > 0)$ 中更精密化,由定理 10.3 已知可將全體有理素數依 $\left(\frac{\Delta}{p}\right) = 0, +1, -1$ 而分爲三類. 以 q 表適合 $\left(\frac{\Delta}{q}\right) = 1$ 之素數,則 $q = \mathfrak{Q}\bar{\mathfrak{Q}}$; 以 r 表適合 $\left(\frac{\Delta}{r}\right) = -1$ 的素數,則 r 本身在 $R(\sqrt{D})$ 中卽爲素理想數. 由定理 9.6 可知,若 $q \nmid \alpha$, 則

$$\alpha^{q-1} \equiv 1 \pmod{\mathfrak{Q}}, \tag{1}$$

又若 $r \nmid \alpha$, 則

$$\alpha^{r^2-1} \equiv 1 \pmod{r}. \tag{2}$$

今往證明:

定理 1. 設 q, r 均不等於 2, 若 $q \nmid \alpha$, 則

$$\alpha^{q-1} \equiv 1 \pmod{q}, \tag{3}$$

及若 $r \nmid \alpha$, 則

$$\alpha^{r+1} \equiv N(\alpha) \pmod{r}. \tag{4}$$

顯然 (1),(3) 等價,而由 (4) 可得 (2).

證: 命

$$\alpha = a + b\frac{\Delta+\sqrt{\Delta}}{2},$$

此處 a, b 是有理整數,而命 p 爲任一奇素數,則由 Fermat 定理可得

$$\alpha^p \equiv a^p + b^p\frac{\Delta^p+(\sqrt{\Delta})^p}{2^p} \equiv a + \frac{b}{2}(\Delta + \Delta^{\frac{p-1}{2}}\sqrt{\Delta}) \equiv$$

$$\equiv a + \frac{b}{2}\left(\Delta + \left(\frac{\Delta}{p}\right)\sqrt{\Delta}\right) \pmod{p}.$$

故若 $p = q$, 則

$$\alpha^q \equiv \alpha \pmod{q},$$

卽得 (3) 式;若 $p = r$, 則

$$\alpha^r \equiv \bar{\alpha} \pmod{r},$$

卽得 (4) 式.

今往研究 p 爲奇素數時, Mersenne 數

$$M = M_p = 2^p - 1$$

的性質. 若有 $\Delta > 0$, 使

$$\left(\frac{\Delta}{M}\right) = -1, \tag{5}$$

且在 $R(\sqrt{\Delta})$ 中有一單位數 ε, 適合 $N(\varepsilon) = -1$, 則命

$$r_m = \varepsilon^{2^m} + \varepsilon'^{2^m},$$

其中 ε' 爲 ε 的共軛數.

定理 2. M 爲素數之必要且充分之條件爲

$$r_{p-1} \equiv 0 \pmod{M}. \tag{6}$$

證: 1) 若 M 是一素數. 由 (5) 可知 M 是一 r. 由定理 1 可知

$$\varepsilon^{M+1} \equiv -1 \pmod{M},$$

故

$$\varepsilon^{2^{p-1}} + \varepsilon'^{2^{p-1}} = \varepsilon'^{2^{p-1}}(\varepsilon^{2^p} + 1) \equiv$$

$$\equiv \varepsilon'^{2^{p-1}}(\varepsilon^{M+1} + 1) \equiv 0 \pmod{M}.$$

2) 假定 M 非素數,則 M 可分解爲

$$M = q_1 \cdots q_s r_1 \cdots r_t.$$

由於 (5) 的關係,故 M 的素因子中必至少有一 r 存在. 因 $M|r_{p-1}$, 可知

$$\varepsilon^{2^{p-1}} + \varepsilon'^{2^{p-1}} \equiv 0 \pmod{M},$$

卽得

$$\varepsilon^{2^p} \equiv -1 \pmod{M}, \tag{7}$$

平方之可得

$$\varepsilon^{2^{p+1}} \equiv 1 \pmod{M}. \tag{8}$$

命 $\mathfrak{P}$ 是 M 的一個素理想數因子,而命 l 表最小的正整數使

$$\varepsilon^l \equiv 1 \pmod{\mathfrak{P}}$$

者,則由 (8) 式可知 $l|2^{p+1}$, 而由 (7) 可知 $l = 2^{p+1}$.

若 $\mathfrak{P}$ 是某一個 q 的因子,則由定理 1 已知

$$\varepsilon^{q-1} \equiv 1 \pmod{\mathfrak{P}},$$

故 $2^{p+1}|q-1$, 但 q 是 M 的因子,不能大於 M, 故此式不可能.

若 $\mathfrak{P}$ 是某一個 r, 再由定理 1 可知

$$\varepsilon^{r+1} \equiv -1 \pmod{r},$$

卽得

$$2^{p+1} \mid 2(r+1),$$

故

$$r = 2^p m - 1.$$

因 $r \leqslant M$, 所以必須 $m = 1$, $r = M$, 卽 M 爲一素數.

例. 取 $\Delta = 5$, $\varepsilon = \frac{1}{2}(1+\sqrt{5})$. 因而得出

$$r_{p-1} = \left(\frac{1}{2}(1+\sqrt{5})\right)^{2^{p-1}} + \left(\frac{1}{2}(1-\sqrt{5})\right)^{2^{p-1}}.$$

若取 $p = 7$, $M_p = 127$, r_m $(m = 1, 2, 3, 4, 5, 6)$ 對模 127 之剩餘爲

$$3,\ 7,\ 47,\ 48,\ 16,\ 0,$$

故 127 是素數. 當然對這一具體問題,本判斷條件並未顯示其效力. 但在證明 687 位數 $M_{2281} = 2^{2281} - 1$ 是素數時,此定理顯出其作用,雖然仍需異常冗長之計算,惟此種計算已歸入用計算機可以算出之範疇. 在數論中找出大的 Mersenne 數是否是素數,一般卽用此類方法.

§ 17. 不定方程.

代數數論之重要進展之一 —— 理想數之創造乃研究 Fermat 問題之產物.

對數學之發展而言,此一概念之獲得實遠重要於解決一個難題. 命 p 爲奇素數, $\rho = e^{2\pi i/p}$. 若能證明在域 $R(\rho)$ 中並無整數使

$$\xi^p + \eta^p + \zeta^p = 0, \quad \xi\eta\zeta \neq 0, \tag{1}$$

則 Fermat 定理當然成立. 而在 $R(\rho)$ 中 $\xi^p + \eta^p$ 可以分解爲一次式,故問題較易入手. 此即 Kummer 研究 Fermat 問題之起點,但主要難點在於整數之唯一分解定理不復存在,Kummer 即由此而創造出理想數論,演變至今,已成爲數學中不可缺少的重要觀念.

欲了解 Kummer 之方法並不簡單,即若假定 $R(\rho)$ 中唯一分解定理成立也必需 Kummer 之一深刻定理才能解決 Fermat 問題. 該定理爲: $R(\rho)$ 中之一個單位數 ε 是另一單位之 p 次冪之必要且充分條件爲 ε 與一有理數對模 $(1-\rho)^p$ 爲同餘. 因此本書中僅能舉兩個極簡單的例子而已.

定理 1. 在 $R(\sqrt{-1})$ 中並無整數使

$$\xi^4 + \eta^4 = \tau^2, \quad \xi\eta\tau \neq 0. \tag{1}$$

證: 在域 $R(\sqrt{-1})$ 中唯一分解定理眞確,即任一理想數都是主理想數,因此不失普遍性可以假定 $(\xi, \eta) = 1$.

1) 命 $\lambda = 1 - i$, 則 λ 是一不可分解數,而 $\lambda^2 = -2i$ 與 $2 = i(1-i)^2$ 相結合. 又由於 $N(2) = 4$, 故 $R(\sqrt{-1})$ 內之整數必與以下四數之一同餘, mod 2

$$0, 1, i, 1-i.$$

由於 $0, 1-i$ 是 λ 之倍數,故任一非 λ 之倍數之整數 α 必適合於

$$\alpha \equiv 1 \text{ 或 } i \pmod{\lambda^2},$$

即

$$\alpha = 1 + \beta\lambda^2 \text{ 或 } \alpha = i + \beta\lambda^2,$$

故有

$$\alpha^4 \equiv 1 \pmod{\lambda^6}. \tag{2}$$

今往證明若有整數 ξ, η, τ 適合 (1) 式,則 ξ, η 中必有一爲 λ 之倍數,蓋若不然,由 (2) 及 (1) 可知

$$2 \equiv \tau^2 \pmod{\lambda^6},$$

由 $2 = \lambda^2 i$, 故 $\lambda | \tau$, 命 $\tau = \lambda\gamma$, 則必 $\lambda \nmid \gamma$, 且有

$$i\lambda^2 \equiv \lambda^2\gamma^2 \pmod{\lambda^6},$$

卽

$$\gamma^2 \equiv i \pmod{\lambda^4},$$

平方之並由 (2) 式可知

$$1 \equiv \gamma^4 \equiv -1 \pmod{\lambda^4}.$$

但此乃不可能之事，故 ξ, η 中必有一爲 λ 之倍數. 又由於對稱關係，故不妨假定 $\lambda|\xi$. 命 $\xi = \lambda^n\delta$, $n \geqslant 1$, $\lambda \nmid \delta$, 如此得出

$$\lambda^{4n}\delta^4 = \tau^2 - \eta^4, \quad n \geqslant 1, \quad \lambda \nmid \delta\eta, \quad (\delta, \eta) = 1.$$

2) 今往證明更一般的定理. $R(\sqrt{-1})$ 中無整數 δ, τ, η 使

$$\varepsilon\lambda^{4n}\delta^4 = \tau^2 - \eta^4, \quad \varepsilon \text{ 爲單位數}, \quad \lambda \nmid \delta\eta, \quad (\delta, \eta) = 1, \quad n \geqslant 1. \tag{3}$$

證明分如下二步: 第一步: 若 (3) 式有解，則必須 $n \geqslant 2$; 第二步: 若 (3) 式對 n 有解，則對 $n-1$ 也有解. 於是得出矛盾的結果，而得定理.

若有整數 δ, τ, η 使 (3) 式成立，則必 $\lambda \nmid \tau$. 又因 $N(\lambda) = 2$, 故 τ 必與 1 同餘, mod λ. 命之爲

$$\tau = 1 + \mu\lambda,$$

平方之得出

$$\tau^2 = 1 + 2\mu\lambda + \mu^2\lambda^2 \equiv 1 + \mu^2\lambda^2 \pmod{\lambda^3}.$$

又由 (2) 式可知

$$\eta^4 \equiv 1 \pmod{\lambda^6}, \tag{4}$$

故由 (3) 得

$$0 \equiv \varepsilon\lambda^{4n}\delta^4 \equiv \tau^2 - \eta^4 \equiv \mu^2\lambda^2 \pmod{\lambda^3},$$

所以必須 $\lambda|\mu$, 故

$$\tau = 1 + \nu\lambda^2, \tag{5}$$

$$\tau^2 = 1 + 2\nu\lambda^2 + \nu^2\lambda^4 = 1 + \lambda^4\nu(i+\nu).$$

由於 ν, $i+\nu$ 成一完全剩餘系, mod λ, 故

$$\nu(i+\nu) \equiv 0 \pmod{\lambda},$$

因此得出

$$\tau^2 \equiv 1 \pmod{\lambda^5}.$$

由 (3) 及 (4) 可知

$$\varepsilon\lambda^{4n}\delta^4 \equiv \tau^2 - \eta^4 \equiv 0 \pmod{\lambda^5},$$

所以必須 $n \geqslant 2$.

今假定 δ, τ, η 適合 (3) 式，而 $n \geqslant 2$, 則得

$$\varepsilon\lambda^{4n}\delta^4 = (\tau - \eta^2)(\tau + \eta^2).$$

由 (5) 式得

$$\tau \equiv 1 \pmod{\lambda^2},$$

另一方面,由於 $\lambda \nmid \eta$, 則得

$$\eta^2 = (1+\kappa\lambda)^2 \equiv 1 \pmod{\lambda^2}. \tag{6}$$

故有

$$\tau - \eta^2 \equiv 0 \pmod{\lambda^2}, \quad \tau + \eta^2 \equiv 2 \equiv 0 \pmod{\lambda^2}.$$

因爲

$$\left(\frac{\tau-\eta^2}{\lambda^2}, \frac{\tau+\eta^2}{\lambda^2}\right) = \left(\frac{\tau-\eta^2}{\lambda^2}, \tau, \eta^2\right) = 1,$$

故從

$$\varepsilon\lambda^{4(n-1)}\delta^4 = \frac{\tau-\eta^2}{\lambda^2}\,\frac{\tau+\eta^2}{\lambda^2} \tag{7}$$

可以得出 $\lambda^{4(n-1)}$ 必須整除此二因子之一. 不妨假定 $\lambda^{4(n-1)}$ 能整除後一因子,蓋若不然,則以 $i\eta$ 代 η 即合所求. 由 (7) 可以得出

$$\frac{\tau-\eta^2}{\lambda^2} = \varepsilon_1\sigma^4, \quad \frac{\tau+\eta^2}{\lambda^2} = \varepsilon_2\lambda^{4(n-1)}\varphi^4 \quad (\lambda \nmid \varphi\sigma, (\sigma, \varphi) = 1),$$

此處 $\varepsilon_1, \varepsilon_2$ 是兩個單位數,故

$$i\eta^2 = \frac{2\eta^2}{\lambda^2} = \varepsilon_2\lambda^{4(n-1)}\varphi^4 - \varepsilon_1\sigma^4,$$

即

$$\eta^2 - \varepsilon_3\sigma^4 = \varepsilon_4\lambda^{4(n-1)}\varphi^4,$$

此處 $\varepsilon_3 = -\frac{\varepsilon_1}{i}$, $\varepsilon_4 = \frac{\varepsilon_2}{i}$ 也是二單位數.

由於 $n \geqslant 2$, $\lambda \nmid \sigma$, 故由 (2) 式可知

$$\eta^2 \equiv \varepsilon_3 \pmod{\lambda^4},$$

由 (6) 得

$$1 \equiv \varepsilon_3 \pmod{\lambda^2},$$

故 ε_3 必須是 $+1$ 或 -1, 而不能是 $\pm i$. 即

$$\varepsilon_4\lambda^{4(n-1)}\varphi^4 = \eta^2 \mp \sigma^4, \quad \lambda \nmid \varphi\sigma, \quad (\varphi, \sigma) = 1,$$

若取上面的負號,則第二步的目的已達,若取下面的正號,則可以 $i\eta$ 代 η, 仍得同樣的結論.

定理 2. 在 $R(\rho)\left(\rho = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}\right)$ 中並無整數 ξ, η, ζ 使

$$\xi^3+\eta^3+\zeta^3=0, \qquad \xi\eta\zeta\neq 0. \tag{8}$$

證: $R(\rho)$ 仍爲一單域,故可假定 $(\xi,\eta)=1$.

1) 命 $\lambda=1-\rho$, 則 $1-\rho^2=-\rho^2(1-\rho)=-\rho^2\lambda$, 而 $N(\lambda)=-\rho^2\lambda^2=3$, 故 λ 是一不可分解數,而所有的整數依 mod λ 而分爲三類,且可以 $0,1,-1$ 表之,故若 $\lambda\nmid\xi$, 則

$$\xi\equiv\pm 1 \pmod{\lambda}.$$

今往證明

$$\xi^3\equiv\pm 1 \pmod{\lambda^4}. \tag{9}$$

若能證明取 + 號之情況卽足,蓋不然可以 $-\xi$ 代 ξ 而得出同樣結果. 命 $\xi=1+\beta\lambda$, 可得

$$\xi^3-1=(\xi-1)(\xi-\rho)(\xi-\rho^2)=\beta\lambda(\beta\lambda+1-\rho)(\beta\lambda+1-\rho^2)=$$
$$=\beta\lambda(\beta\lambda+\lambda)(\beta\lambda-\rho^2\lambda)=\lambda^3\beta(\beta+1)(\beta-\rho^2).$$

由於 $\beta,\beta+1,\beta-\rho^2$ 對 mod λ 互不同餘及 $N(\lambda)=3$, 故此三者間必有一個是 λ 的倍數,因之得到,若 $\lambda\nmid\eta$, 則

$$\eta^3\equiv\pm 1 \pmod{\lambda^4}. \tag{10}$$

今若 $\lambda\nmid\xi\eta\zeta$, 則得

$$0\equiv\xi^3+\eta^3+\zeta^3\equiv\pm1\pm1\pm1 \pmod{\lambda^3}.$$

各種變化僅得 ± 1, ± 3, 無一是 λ^3 的倍數,故 ξ,η,ζ 中必有一爲 λ 所整除. 命之爲

$$\zeta=\lambda^n\gamma, \quad n\geqslant 1, \quad \lambda\nmid\gamma,$$

卽得

$$\xi^3+\eta^3+\lambda^{3n}\gamma^3=0, \qquad (\xi,\eta)=1, \quad \lambda\nmid\gamma, \quad n\geqslant 1.$$

2) 今往證明更一般些的定理. $R(\rho)$ 中無整數 ξ,η,γ 使

$$\xi^3+\eta^3+\varepsilon\lambda^{3n}\gamma^3=0, \quad (\xi,\eta)=1, \quad \lambda\nmid\gamma, \quad n\geqslant 1, \tag{11}$$

此處 ε 是一單位數. 如定理 1, 證明仍分二步: 第一步: 若 (11) 式有解, 則必 $n\geqslant 2$; 第二步: 若 (11) 有解,則以 $n-1$ 代 n 後所得之方程也有解;於是將得到矛盾,而導出定理.

若 (11) 有解,則由 (10) 可知

$$-\varepsilon\lambda^{3n}\gamma^3\equiv\xi^3+\eta^3\equiv\pm1\pm1 \pmod{\lambda^4}.$$

因爲 $+1+1$ 及 $-1-1$ 非 λ 之倍數,故可知

$$-\varepsilon\lambda^{3n}\gamma^3\equiv 0 \pmod{\lambda^4},$$

卽 $n\geqslant 2$.

設 ξ, η, γ 爲 (11) 式的解,因 $1\equiv\rho\equiv\rho^2 \pmod{\lambda}$,所以

$$\xi+\eta\equiv\xi+\rho\eta\equiv\xi+\rho^2\eta \pmod{\lambda},$$

故 $-\varepsilon\lambda^{3n}\gamma^3=\xi^3+\eta^3=(\xi+\eta)(\xi+\rho\eta)(\xi+\rho^2\eta)$ 的三個因子都是 λ 之倍數.

又不難證明 $\frac{\xi+\eta}{\lambda}, \frac{\xi+\rho\eta}{\lambda}, \frac{\xi+\rho^2\eta}{\lambda}$ 兩兩互素,蓋由 $(\xi,\eta)=1$, 及 $\frac{\xi+\eta}{\lambda}-\frac{\xi+\rho\eta}{\lambda}=\eta$, $\rho\frac{\xi+\eta}{\lambda}-\frac{\xi+\rho\eta}{\lambda}=-\xi$, 可得 $\left(\frac{\xi+\eta}{\lambda},\frac{\xi+\rho\eta}{\lambda}\right)=1$, 類似地可以證明 $\left(\frac{\xi+\rho\eta}{\lambda},\frac{\xi+\rho^2\eta}{\lambda}\right)=1$, 及 $\left(\frac{\xi+\rho^2\eta}{\lambda},\frac{\xi+\eta}{\lambda}\right)=1$, 因此

$$-\varepsilon\lambda^{3(n-1)}\gamma^3=\frac{\xi+\eta}{\lambda}\,\frac{\xi+\rho\eta}{\lambda}\,\frac{\xi+\rho^2\eta}{\lambda}$$

之三因子中必有一爲 $\lambda^{3(n-1)}$ 的倍數,不妨假定 $\frac{\xi+\eta}{\lambda}$ 能爲 $\lambda^{3(n-1)}$ 整除(不然,可以 $\rho\eta$ 或 $\rho^2\eta$ 代 η),故得

$$\xi+\eta=\varepsilon_1\lambda^{3n-2}\mu^3,\quad \xi+\rho\eta=\varepsilon_2\lambda\nu^3,\quad \xi+\rho^2\eta=\varepsilon_3\lambda\sigma^3, \tag{12}$$

此處 $\varepsilon_1, \varepsilon_2, \varepsilon_3$ 爲單位數, μ, ν, σ 是兩兩互素的整數,且無一爲 λ 之倍數.

由 (12) 可知

$$0=\xi+\eta+\rho(\xi+\rho\eta)+\rho^2(\xi+\rho^2\eta)=$$
$$=\varepsilon_1\lambda^{3n-2}\mu^3+\rho\varepsilon_2\lambda\nu^3+\rho^2\varepsilon_3\lambda\sigma^3,$$

卽得一形如

$$\nu^3+\varepsilon_4\sigma^3+\varepsilon_5\lambda^{3(n-1)}\mu^3=0,\qquad (\nu,\sigma)=1,\quad \lambda\nmid\mu \tag{13}$$

之方程,此處 $\varepsilon_4, \varepsilon_5$ 也是單位數.

由 (13) 可知

$$\nu^3+\varepsilon_4\sigma^3\equiv 0 \pmod{\lambda^2},$$

再由 (10) 可知

$$\pm 1\pm\varepsilon_4\equiv 0 \pmod{\lambda^2},$$

而各個單位 $\pm 1, \pm\rho, \pm\rho^2$ 中僅有 $\varepsilon_4=\pm 1$ 才能適合此式,故必須 $\varepsilon_4=\pm 1$, 於是 (13) 式又爲 (11) 之形式,但 n 已換爲 $n-1$, 故定理得證.

§18. 表.

在節末的二個附表中給出了所有適合於 $-100 < D \leqslant 100$ 的二次域的整底、基數、域上的理想數類、與理想數類對應的二次型類以及他們的特徵系統等等. 而在第二個表中更給出了 ω 的連分數表示與域內的基本單位數. 詳細言之:

表 I 中第一列的各數爲 D 的數值;第二列爲域 $R(\sqrt{D})$ 中的 ω (ω 的定義見定理 4.6);第三列表示域的基數 Δ; 第四列中各理想數代表域 $R(\sqrt{D})$ 上的理想數類;第五列給出這些類間的相互關係; 第六列中各二次型代表與理想數類對應的二次型類;而第七列則給出這些二次型類的特徵系統.

表 II 中第一列、第二列仍是 D 的數值與 $R(\sqrt{D})$ 中的 ω; 第三列中的各連分數當 D 爲無平方因子數時是 ω 的連分數表示, 而當 D 內含有不等於 1 的平方因子時,則是 $\sqrt{D}$ 的連分數表示; 第四列是域的基數 Δ; 第五列中的 $x+y\sqrt{D}$, 當 D 爲無平方因子數時,是 $R(\sqrt{D})$ 內的基本單位數 η, 而當 D 內含有平方因子時,則是

$$x^2-y^2D=\pm 1$$

的最小正整數解 (若 $x^2-y^2D=-1$ 有解,則 $x+y\sqrt{D}$ 適合 $x^2-y^2D=-1$. 不然 x, y 適合 $x^2-y^2D=+1$); 第六列是 $N(x+y\sqrt{D})$; 第七列是域 $R(\sqrt{D})$ 上的理想數類 (非狹義的); 第八列表出了各類間的關係;第九列給出了與理想數類對應的二次型;第十列給出了二次型類的特徵系統.

表 I

D	ω	Δ	理想數	類	二次型	特徵系統
-1	$\sqrt{-1}$	-2^2	(1)	1	x^2+y^2	$+1$
-2	$\sqrt{-2}$	-2^3	(1)	1	$2x^2+y^2$	$+1$
-3	$\frac{1+\sqrt{-3}}{2}$	-3	(1)	1	x^2+xy+y^2	$+1$
-5	$\sqrt{-5}$	$-2^2\cdot 5$	(1)	A^2	$5x^2+y^2$	$+1,+1$
			$(2,1+\sqrt{-5})$	A	$3x^2+2xy+2y^2$	$-1,-1$
-6	$\sqrt{-6}$	$-2^3\cdot 3$	(1)	A^2	$6x^2+y^2$	$+1,+1$
			$(2,\sqrt{-6})$	A	$3x^2+2y^2$	$-1,-1$
-7	$\frac{1+\sqrt{-7}}{2}$	-7	(1)	1	$2x^2+xy+y^2$	$+1$
-10	$\sqrt{-10}$	$-5\cdot 2^3$	(1)	A^2	$10x^2+y^2$	$+1,+1$
			$(2,\sqrt{-10})$	A	$5x^2+2y^2$	$-1,-1$
-11	$\frac{1+\sqrt{-11}}{2}$	-11	(1)	1	$3x^2+xy+y^2$	$+1$
-13	$\sqrt{-13}$	$-2^2\cdot 13$	(1)	A^2	$13x^2+y^2$	$+1,+1$
			$(2,1+\sqrt{-13})$	A	$7x^2+2xy+2y^2$	$-1,-1$
-14	$\sqrt{-14}$	$-7\cdot 2^3$	(1)	I^4	$14x^2+y^2$	$+1,+1$
			$(3,2+\sqrt{-14})$	I^3	$6x^2+4xy+3y^2$	$-1,-1$
			$(2,\sqrt{-14})$	I^2	$7x^2+2y^2$	$+1,+1$
			$(3,1+\sqrt{-14})$	I	$5x^2+2xy+3y^2$	$-1,-1$
-15	$\frac{1+\sqrt{-15}}{2}$	$-3\cdot 5$	(1)	A^2	$4x^2+xy+y^2$	$+1,+1$
			$(2,1+\omega)$	A	$3x^2+3xy+2y^2$	$-1,-1$
-17	$\sqrt{-17}$	$-2^2\cdot 17$	(1)	I^4	$17x^2+y^2$	$+1,+1$
			$(3,2+\sqrt{-17})$	I^3	$7x^2+4xy+3y^2$	$-1,-1$
			$(2,1+\sqrt{-17})$	I^2	$9x^2+2xy+2y^2$	$+1,+1$
			$(3,1+\sqrt{-17})$	I	$6x^2+2xy+3y^2$	$-1,-1$
-19	$\frac{1+\sqrt{-19}}{2}$	-19	(1)	1	$5x^2+xy+y^2$	$+1$
-21	$\sqrt{-21}$	$-3\cdot 2^2\cdot 7$	(1)	$A^2A_1^2$	$+21x^2+y^2$	$+1,+1,+1$
			$(5,3+\sqrt{-21})$	AA_1	$6x^2+6xy+5y^2$	$-1,-1,+1$
			$(3,\sqrt{-21})$	A_1	$7x^2+3y^2$	$+1,-1,-1$
			$(2,1+\sqrt{-21})$	A	$11x^2+2xy+2y^2$	$-1,+1,-1$

表 I (續)

D	ω	Δ	理想數	類	二次型	特徵系統
-22	$\sqrt{-22}$	$-2^3\cdot 11$	(1)	A^2	$22x^2+y^2$	$+1,+1$
			$(2,\sqrt{-22})$	A	$11x^2+2y^2$	$-1,-1$
-23	$\frac{1+\sqrt{-23}}{2}$	-23	(1)	J^3	$6x^2+xy+y^2$	$+1$
			$\left(2,1+\frac{1+\sqrt{-23}}{2}\right)$	J^2	$4x^2+3xy+2y^2$	$+1$
			$\left(2,\frac{1+\sqrt{-23}}{2}\right)$	J	$3x^2+2xy+2y^2$	$+1$
-26	$\sqrt{-26}$	$-2^3\cdot 13$	(1)	J^6	$26x^2+y^2$	$+1,+1$
			$(5,3+\sqrt{-26})$	J^5	$7x^2+6xy+5y^2$	$-1,-1$
			$(3,1+\sqrt{-26})$	J^4	$9x^2+2xy+3y^2$	$+1,+1$
			$(2,\sqrt{-26})$	J^3	$13x^2+2y^2$	$-1,-1$
			$(3,2+\sqrt{-26})$	J^2	$10x^2+4xy+3y^2$	$+1,+1$
			$(5,2+\sqrt{-26})$	J	$6x^2+4xy+5y^2$	$-1,-1$
-29	$\sqrt{-29}$	$-2^2\cdot 29$	(1)	J^6	$29x^2+y^2$	$+1,+1$
			$(3,2+\sqrt{-29})$	J^5	$11x^2+4xy+3y^2$	$-1,-1$
			$(5,4+\sqrt{-29})$	J^4	$9x^2+8xy+5y^2$	$+1,+1$
			$(2,1+\sqrt{-29})$	J^3	$15x^2+2xy+2y^2$	$-1,-1$
			$(5,1+\sqrt{-29})$	J^2	$6x^2+2xy+5y^2$	$+1,+1$
			$(3,1+\sqrt{-29})$	J	$10x^2+2xy+3y^2$	$-1,-1$
-30	$\sqrt{-30}$	$-2^3\cdot 3\cdot 5$	(1)	$A^2A_1^2$	$30x^2+y^2$	$+1,+1,+1$
			$(2,\sqrt{-30})$	AA_1	$15x^2+2y^2$	$-1,-1,+1$
			$(3,\sqrt{-30})$	A_1	$10x^2+3y^2$	$+1,-1,-1$
			$(5,\sqrt{-30})$	A	$6x^2+5y^2$	$-1,+1,-1$
-31	$\frac{1}{2}(1+\sqrt{-31})$	-31	(1)	J^3	$8x^2+xy+y^2$	$+1$
			$(2,\omega)$	J^2	$4x^2+xy+2y^2$	$+1$
			$(2,1+\omega)$	J	$5x^2+3xy+2y^2$	$+1$
-33	$\sqrt{-33}$	$-2^2\cdot 3\cdot 11$	(1)	$A^2A_1^2$	$33x^2+y^2$	$+1,+1,+1$
			$(2,1+\sqrt{-33})$	AA_1	$17x^2+2xy+2y^2$	$-1,-1,+1$
			$(3,\sqrt{-33})$	A_1	$11x^2+3y^2$	$-1,+1,-1$
			$(6,3+\sqrt{-33})$	A	$7x^2+6xy+6y^2$	$+1,-1,-1$
-34	$\sqrt{-34}$	$-2^3 17$	(1)	J^4	$34x^2+y^2$	$+1,+1$
			$(5,4+\sqrt{-34})$	J^3	$10x^2+8xy+5y^2$	$-1,-1$

表 I (續)

D	ω	Δ	理 想 數	類	二 次 型	特徵系統
-34			$(2,\sqrt{-34})$	I^2	$17x^2+2y^2$	$+1,+1$
			$(5,1+\sqrt{-34})$	I	$7x^2+2xy+5y^2$	$-1,-1$
-35	$\frac{1}{2}(1+\sqrt{-35})$	$-5\cdot7$	(1)	A^2	$9x^2+xy+y^2$	$+1,+1$
			$\left(5,\frac{5+\sqrt{-35}}{2}\right)$	A	$3x^2+5xy+5y^2$	$-1,-1$
-37	$\sqrt{-37}$	$-2^2\cdot37$	(1)	A^2	$37x^2+y^2$	$+1,+1$
			$(2,1+\sqrt{-37})$	A	$19x^2+2xy+2y^2$	$-1,-1$
-38	$\sqrt{-38}$	$-2^3\cdot19$	(1)	I^6	$38x^2+y^2$	$+1,+1$
			$(3,2+\sqrt{-38})$	I^5	$14x^2+4xy+3y^2$	$-1,-1$
			$(7,2+\sqrt{-38})$	I^4	$6x^2+4xy+7y^2$	$+1,+1$
			$(2,\sqrt{-38})$	I^3	$19x^2+2y^2$	$-1,-1$
			$(7,5+\sqrt{-38})$	I^2	$9x^2+10xy+7y^2$	$+1,+1$
			$(3,1+\sqrt{-38})$	I	$13x^2+2xy+3y^2$	$-1,-1$
-39	$\frac{1}{2}(1+\sqrt{-39})$	$-3\cdot13$	(1)	I^4	$10x^2+xy+y^2$	$+1,+1$
			$(2,1+\omega)$	I^3	$6x^2+3xy+2y^2$	$-1,-1$
			$(3,1+\omega)$	I^2	$4x^2+3xy+3y^2$	$+1,+1$
			$(2,\omega)$	I	$5x^2+xy+2y^2$	$-1,-1$
-41	$\sqrt{-41}$	$-2^2\cdot41$	(1)	I^8	$41x^2+y^2$	$+1,+1$
			$(3,2+\sqrt{-41})$	I^7	$15x^2+4xy+3y^2$	$-1,-1$
			$(5,3+\sqrt{-41})$	I^6	$10x^2+6xy+5y^2$	$+1,+1$
			$(7,6+\sqrt{-41})$	I^5	$11x^2+12xy+7y^2$	$-1,-1$
			$(2,1+\sqrt{-41})$	I^4	$21x^2+2xy+2y^2$	$+1,+1$
			$(7,1+\sqrt{-41})$	I^3	$6x^2+2xy+7y^2$	$-1,-1$
			$(5,2+\sqrt{-41})$	I^2	$9x^2+4xy+5y^2$	$+1,+1$
			$(3,1+\sqrt{-41})$	I	$14x^2+2xy+3y^2$	$-1,-1$
-42	$\sqrt{-42}$	$-3\cdot2^3\cdot7$	(1)	$A^2A_1^2$	$42x^2+y^2$	$+1,+1,+1$
			$(7,\sqrt{-42})$	AA_1	$6x^2+7y^2$	$+1,-1,-1$
			$(3,\sqrt{-42})$	A_1	$14x^2+3y^2$	$-1,-1,+1$
			$(2,\sqrt{-42})$	A	$21x^2+2y^2$	$-1,+1,-1$
-43	$\frac{1}{2}(1+\sqrt{-43})$	-43	(1)	1	$11x^2+xy+y^2$	$+1$

表 I (續)

D	ω	Δ	理想數	類	二次型	特徵系統
-46	$\sqrt{-46}$	$-2^3\cdot 23$	(1)	I^4	$46x^2+y^2$	$+1,+1$
			$(5,3+\sqrt{-46})$	I^3	$11x^2+6xy+5y^2$	$-1,-1$
			$(2,\sqrt{-46})$	I^2	$23x^2+2y^2$	$+1,+1$
			$(5,2+\sqrt{-46})$	I	$10x^2+4xy+5y^2$	$-1,-1$
-47	$\frac{1}{2}(1+\sqrt{-47})$	-47	(1)	I^5	$12x^2+xy+y^2$	$+1$
			$(2,\omega)$	I^4	$6x^2+xy+2y^2$	$+1$
			$(3,2+\omega)$	I^3	$6x^2+5xy+3y^2$	$+1$
			$(3,\omega)$	I^2	$4x^2+xy+3y^2$	$+1$
			$(2,1+\omega)$	I	$7x^2+3xy+2y^2$	$+1$
-51	$\frac{1}{2}(1+\sqrt{-51})$	$-3\cdot 17$	(1)	A^2	$13x^2+xy+y^2$	$+1,+1$
			$(3,1+\omega)$	A	$5x^2+3xy+3y^2$	$-1,-1$
-53	$\sqrt{-53}$	$-2^2\cdot 53$	(1)	I^6	$53x^2+y^2$	$+1,+1$
			$(3,2+\sqrt{-53})$	I^5	$19x^2+4xy+3y^2$	$-1,-1$
			$(9,8+\sqrt{-53})$	I^4	$13x^2+16xy+9y^2$	$+1,+1$
			$(2,1+\sqrt{-53})$	I^3	$27x^2+2xy+2y^2$	$-1,-1$
			$(9,1+\sqrt{-53})$	I^2	$6x^2+2xy+9y^2$	$+1,+1$
			$(3,1+\sqrt{-53})$	I	$18x^2+2xy+3y^2$	$-1,-1$
-55	$\frac{1}{2}(1+\sqrt{-55})$	$-5\cdot 11$	(1)	I^4	$14x^2+xy+y^2$	$+1,+1$
			$(2,1+\omega)$	I^3	$8x^2+3xy+2y^2$	$-1,-1$
			$(5,2+\omega)$	I^2	$4x^2+5xy+5y^2$	$+1,+1$
			$(2,\omega)$	I	$7x^2+xy+2y^2$	$-1,-1$
-57	$\sqrt{-57}$	$-3\cdot 2^2\cdot 19$	(1)	$A^2A_1^2$	$57x^2+y^2$	$+1,+1,+1$
			$(2,1+\sqrt{-57})$	AA_1	$29x^2+2xy+2y^2$	$-1,-1,+1$
			$(3,\sqrt{-57})$	A_1	$19x^2+3y^2$	$+1,-1,-1$
			$(6,3+\sqrt{-57})$	A	$11x^2+6xy+6y^2$	$-1,+1,-1$
-58	$\sqrt{-58}$	$-2^3\cdot 29$	(1)	A^2	$58x^2+y^2$	$+1,+1$
			$(2,\sqrt{-58})$	A	$29x^2+2y^2$	$-1,-1$
-59	$\frac{1}{2}(1+\sqrt{-59})$	-59	(1)	I^3	$15x^2+xy+y^2$	$+1$
			$\left(3,\frac{5+\sqrt{-59}}{2}\right)$	I^2	$7x^2+5xy+3y^2$	$+1$

表 I (續)

D	ω	Δ	理想數	類	二次型	特徵系統
-59			$\left(3, \frac{1+\sqrt{-59}}{2}\right)$	I	$5x^2+xy+3y^2$	$+1$
-61	$\sqrt{-61}$	$-2^2\cdot 61$	(1)	I^3	$61x^2+y^2$	$+1, +1$
			$(5, 3+\sqrt{-61})$	I^2	$14x^2+6xy+5y^2$	$+1, +1$
			$(5, 2+\sqrt{-61})$	I	$13x^2+4xy+5y^2$	$+1, +1$
			$(7, 4+\sqrt{-61})$	AI^2	$11x^2+8xy+7y^2$	$-1, -1$
			$(7, 3+\sqrt{-61})$	AI	$10x^2+6xy+7y^2$	$-1, -1$
			$(2, 1+\sqrt{-61})$	A	$31x^2+2xy+2y^2$	$-1, -1$
-62	$\sqrt{-62}$	$-2^3\cdot 31$	(1)	I^8	$62x^2+y^2$	$+1, +1$
			$(3, 2+\sqrt{-62})$	I^7	$22x^2+4xy+3y^2$	$-1, -1$
			$(7, 1+\sqrt{-62})$	I^6	$9x^2+2xy+7y^2$	$+1, +1$
			$(11, 2+\sqrt{-62})$	I^5	$6x^2+4xy+11y^2$	$-1, -1$
			$(2, \sqrt{-62})$	I^4	$31x^2+2y^2$	$+1, +1$
			$(11, 9+\sqrt{-62})$	I^3	$13x^2+18xy+11y^2$	$-1, -1$
			$(7, 6+\sqrt{-62})$	I^2	$14x^2+12xy+7y^2$	$+1, +1$
			$(3, 1+\sqrt{-62})$	I	$21x^2+2xy+3y^2$	$-1, -1$
-65	$\sqrt{-65}$	$-2^2\cdot 5\cdot 13$	(1)	I^4	$65x^2+y^2$	$+1, +1, +1$
			$(3, 2+\sqrt{-65})$	I^3	$23x^2+4xy+3y^2$	$-1, +1, -1$
			$(9, 4+\sqrt{-65})$	I^2	$9x^2+8xy+9y^2$	$+1, +1, +1$
			$(3, 1+\sqrt{-65})$	I	$22x^2+2xy+3y^2$	$-1, +1, -1$
			$(11, 10+\sqrt{-65})$	AI^3	$15x^2+20xy+11y^2$	$+1, -1, -1$
			$(2, 1+\sqrt{-65})$	AI^2	$33x^2+2xy+2y^2$	$-1, -1, +1$
			$(11, 1+\sqrt{-65})$	AI	$6x^2+2xy+11y^2$	$+1, -1, -1$
			$(5, \sqrt{-65})$	A	$13x^2+5y^2$	$-1, -1, +1$
-66	$\sqrt{-66}$	$-2^3\cdot 3\cdot 11$	(1)	I^4	$66x^2+y^2$	$+1, +1, +1$
			$(5, 3+\sqrt{-66})$	I^3	$15x^2+6xy+5y^2$	$-1, +1, -1$
			$(3, \sqrt{-66})$	I^2	$22x^2+3y^2$	$+1, +1, +1$
			$(5, 2+\sqrt{-66})$	I	$14x^2+4xy+5y^2$	$-1, +1, -1$
			$(7, 2+\sqrt{-66})$	AI^3	$10x^2+4xy+7y^2$	$+1, -1, -1$
			$(11, \sqrt{-66})$	AI^2	$6x^2+11y^2$	$-1, -1, +1$

表 I (續)

D	ω	Δ	理想數	類	二次型	特徵系統
-66			$(7,5+\sqrt{-66})$	AJ	$13x^2+10xy+7y^2$	$+1,-1,-1$
			$(2,\sqrt{-66})$	A	$33x^2+2y^2$	$-1,-1,+1$
-67	$\frac{1}{2}(1+\sqrt{-67})$	-67	(1)	1	$17x^2+xy+y^2$	$+1$
-69	$\sqrt{-69}$	$-2^2\cdot3\cdot23$	(1)	J^4	$69x^2+y^2$	$+1,+1,+1$
			$(7,6+\sqrt{-69})$	J^3	$15x^2+12xy+7y^2$	$+1,-1,-1$
			$(6,3+\sqrt{-69})$	J^2	$13x^2+6xy+6y^2$	$+1,+1,+1$
			$(7,1+\sqrt{-69})$	J	$10x^2+2xy+7y^2$	$+1,-1,-1$
			$(5,1+\sqrt{-69})$	AJ^3	$14x^2+2xy+5y^2$	$-1,-1,+1$
			$(3,\sqrt{-69})$	AJ^2	$23x^2+3y^2$	$-1,+1,-1$
			$(5,4+\sqrt{-69})$	AJ	$17x^2+8xy+5y^2$	$-1,-1,+1$
			$(2,1+\sqrt{-69})$	A	$35x^2+2xy+2y^2$	$-1,+1,-1$
-70	$\sqrt{-70}$	$-2^2\cdot5\cdot7$	(1)	$A^2A_1^2$	$70x^2+y^2$	$+1,+1,+1$
			$(7,\sqrt{-70})$	AA_1	$10x^2+7y^2$	$-1,-1,+1$
			$(5,\sqrt{-70})$	A_1	$14x^2+5y^2$	$+1,-1,-1$
			$(2,\sqrt{-70})$	A	$35x^2+2y^2$	$-1,+1,-1$
-71	$\frac{1}{2}(1+\sqrt{-71})$	-71	(1)	J^7	$71x^2+y^2$	$+1$
			$\left(2,\frac{3+\sqrt{-71}}{2}\right)$	J^6	$10x^2+3xy+2y^2$	$+1$
			$\left(5,\frac{7+\sqrt{-71}}{2}\right)$	J^5	$6x^2+7xy+5y^2$	$+1$
			$\left(3,\frac{5+\sqrt{-71}}{2}\right)$	J^4	$8x^2+5xy+3y^2$	$+1$
			$\left(3,\frac{1+\sqrt{-71}}{2}\right)$	J^3	$6x^2+xy+3y^2$	$+1$
			$\left(5,\frac{3+\sqrt{-71}}{2}\right)$	J^2	$4x^2+3xy+5y^2$	$+1$
			$\left(2,\frac{1+\sqrt{-71}}{2}\right)$	J	$9x^2+xy+2y^2$	$+1$
-73	$\sqrt{-73}$	$-2^2\cdot73$	(1)	J^4	$73x^2+y^2$	$+1,+1$
			$(7,5+\sqrt{-73})$	J^3	$14x^2+10xy+7y^2$	$-1,-1$
			$(2,1+\sqrt{-73})$	J^2	$37x^2+2xy+2y^2$	$+1,+1$
			$(7,2+\sqrt{-73})$	J	$11x^2+4xy+7y^2$	$-1,-1$

表 I (續)

D	ω	Δ	理想數	類	二次型	特徵系統
-74	$\sqrt{-74}$	$-2^2\cdot 37$	(1)	J^5	$74x^2+y^2$	$+1, +1$
			$(11, 6+\sqrt{-74})$	J^4	$10x^2+12xy+11y^2$	$+1, +1$
			$(3, 1+\sqrt{-74})$	J^3	$25x^2+2xy+3y^2$	$+1, +1$
			$(3, 2+\sqrt{-74})$	J^2	$26x^2+4xy+3y^2$	$+1, +1$
			$(11, 5+\sqrt{-74})$	J	$9x^2+10xy+11y^2$	$+1, +1$
			$(5, 4+\sqrt{-74})$	AJ^4	$18x^2+8xy+5y^2$	$-1, -1$
			$(6, 4+\sqrt{-74})$	AJ^3	$15x^2+8xy+6y^2$	$-1, -1$
			$(6, 2+\sqrt{-74})$	AJ^2	$13x^2+4xy+6y^2$	$-1, -1$
			$(5, 1+\sqrt{-74})$	AJ	$15x^2+2xy+5y^2$	$-1, -1$
			$(2, \sqrt{-74})$	A	$37x^2+2y^2$	$-1, -1$
-77	$\sqrt{-77}$	$-2^2\cdot 7\cdot 11$	(1)	J^4	$77x^2+y^2$	$+1, +1, +1$
			$(3, 2+\sqrt{-77})$	J^3	$27x^2+4xy+3y^2$	$-1, +1, -1$
			$(14, 7+\sqrt{-77})$	J^2	$9x^2+14xy+14y^2$	$+1, +1, +1$
			$(3, 1+\sqrt{-77})$	J	$26x^2+2xy+3y^2$	$-1, +1, -1$
			$(6, 5+\sqrt{-77})$	AJ^3	$17x^2+10xy+6y^2$	$-1, -1, +1$
			$(7, \sqrt{-77})$	AJ^2	$11x^2+7y^2$	$+1, -1, -1$
			$(6, 1+\sqrt{-77})$	AJ	$13x^2+2xy+6y^2$	$-1, -1, +1$
			$(2, 1+\sqrt{-77})$	A	$39x^2+2xy+2y^2$	$+1, -1, -1$
-78	$\sqrt{-78}$	$-2^3\cdot 3\cdot 13$	(1)	$A^2A_1^2$	$78x^2+y^2$	$+1, +1, +1$
			$(2, \sqrt{-78})$	AA_1	$39x^2+2y^2$	$-1, -1, +1$
			$(13, \sqrt{-78})$	A_1	$6x^2+13y^2$	$+1, -1, -1$
			$(3, \sqrt{-78})$	A	$26x^2+3y^2$	$-1, +1, -1$
-79	$\frac{1}{2}(1+\sqrt{-79})$	-79	(1)	J^5	$20x^2+xy+y^2$	$+1$
			$\left(2, \frac{1+\sqrt{-79}}{2}\right)$	J^4	$10x^2+xy+2y^2$	$+1$
			$\left(5, \frac{9+\sqrt{-79}}{2}\right)$	J^3	$8x^2+9xy+5y^2$	$+1$
			$\left(5, \frac{1+\sqrt{-79}}{2}\right)$	J^2	$4x^2+xy+5y^2$	$+1$
			$\left(2, \frac{3+\sqrt{-79}}{2}\right)$	J	$11x^2+3xy+2y^2$	$+1$

表 I (續)

D	ω	Δ	理想數	類	二次型	特徵系統
-82	$\sqrt{-82}$	$-2^3\cdot 41$	(1)	J^4	$82x^2+y^2$	$+1,+1$
			$(7,4+\sqrt{-82})$	J^3	$14x^2+8xy+7y^2$	$-1,-1$
			$(2,\sqrt{-82})$	J^2	$41x^2+2y^2$	$+1,+1$
			$(7,3+\sqrt{-82})$	J	$13x^2+6xy+7y^2$	$-1,-1$
-83	$\frac{1}{2}(1+\sqrt{-83})$	-83	(1)	J^3	$21x^2+xy+y^2$	$+1$
			$\left(3,\frac{5+\sqrt{-83}}{2}\right)$	J^2	$9x^2+5xy+3y^2$	$+1$
			$\left(3,\frac{1+\sqrt{-83}}{2}\right)$	J	$7x^2+xy+3y^2$	$+1$
-85	$\sqrt{-85}$	$-2^2\cdot 5\cdot 17$	(1)	$A^2A_1^2$	$85x^2+y^2$	$+1,+1,+1$
			$(5,\sqrt{-85})$	AA_1	$17x^2+5y^2$	$-1,-1,+1$
			$(10,5+\sqrt{-85})$	A_1	$11x^2+10xy+10y^2$	$+1,-1,-1$
			$(2,1+\sqrt{-85})$	A	$43x^2+2xy+2y^2$	$-1,+1,-1$
-86	$\sqrt{-86}$	$-2^3\cdot 43$	(1)	J^{10}	$86x^2+y^2$	$+1,+1$
			$(3,2+\sqrt{-86})$	J^9	$30x^2+4xy+3y^2$	$-1,-1$
			$(9,2+\sqrt{-86})$	J^8	$10x^2+4xy+9y^2$	$+1,+1$
			$(5,2+\sqrt{-86})$	J^7	$18x^2+4xy+5y^2$	$-1,-1$
			$(17,13+\sqrt{-86})$	J^6	$15x^2+26xy+17y^2$	$+1,+1$
			$(2,\sqrt{-86})$	J^5	$43x^2+2,$	$-1,-1$
			$(17,4+\sqrt{-86})$	J^4	$6x^2+8xy+17y^2$	$+1,+1$
			$(5,3+\sqrt{-86})$	J^3	$19x^2+6xy+5y^2$	$-1,-1$
			$(9,7+\sqrt{-86})$	J^2	$15x^2+14xy+9y^2$	$+1,+1$
			$(3,1+\sqrt{-86})$	J	$29x^2+2xy+3y^2$	$-1,-1$
-87	$\frac{1}{2}(1+\sqrt{-87})$	$-3\cdot 29$	(1)	J^6	$22x^2+xy+y^2$	$+1,+1$
			$\left(2,\frac{3+\sqrt{-87}}{2}\right)$	J^5	$12x^2+3xy+2y^2$	$-1,-1$
			$\left(7,\frac{5+\sqrt{-87}}{2}\right)$	J^4	$4x^2+5xy+7y^2$	$+1,+1$
			$\left(3,\frac{3+\sqrt{-87}}{2}\right)$	J^3	$8x^2+3xy+3y^2$	$-1,-1$
			$\left(7,\frac{9+\sqrt{-87}}{2}\right)$	J^2	$6x^2+9xy+7y^2$	$+1,+1$

表 I (續)

D	ω	Δ	理想數	類	二次型	特徵系統
-87			$\left(2,\frac{1+\sqrt{-87}}{2}\right)$	J	$11x^2+xy+2y^2$	$-1,-1$
-89	$\sqrt{-89}$	$-2^2\cdot 89$	(1)	J^{12}	$89x^2+y^2$	$+1,+1$
			$(3,2+\sqrt{-89})$	J^{11}	$31x^2+4xy+3y^2$	$-1,-1$
			$(17,9+\sqrt{-89})$	J^{10}	$10x^2+18xy+17y^2$	$+1,+1$
			$(7,3+\sqrt{-89})$	J^9	$14x^2+6xy+7y^2$	$-1,-1$
			$(5,4+\sqrt{-89})$	J^8	$21x^2+8xy+5y^2$	$+1,+1$
			$(6,1+\sqrt{-89})$	J^7	$15x^2+2xy+6y^2$	$-1,-1$
			$(2,1+\sqrt{-89})$	J^6	$45x^2+2xy+2y^2$	$+1,+1$
			$(6,5+\sqrt{-89})$	J^5	$19x^2+10xy+6y^2$	$-1,-1$
			$(5,1+\sqrt{-89})$	J^4	$18x^2+2xy+5y^2$	$+1,+1$
			$(7,4+\sqrt{-89})$	J^3	$15x^2+8xy+7y^2$	$-1,-1$
			$(17,8+\sqrt{-89})$	J^2	$9x^2+16xy+17y^2$	$+1,+1$
			$(3,1+\sqrt{-89})$	J	$30x^2+2xy+3y^2$	$-1,-1$
-91	$\frac{1+\sqrt{-91}}{2}$	$-7\cdot 13$	(1)	A^2	$23x^2+xy+y^2$	$+1,+1$
			$\left(7,\frac{7+\sqrt{-91}}{2}\right)$	A	$5x^2+7xy+7y^2$	$-1,-1$
-93	$\sqrt{-93}$	$-2^2\cdot 3\cdot 31$	(1)	$A^2A_1^2$	$93x^2+y^2$	$+1,+1,+1$
			$(6,3+\sqrt{-93})$	AA_1	$17x^2+6xy+6y^2$	$-1,-1,+1$
			$(3,\sqrt{-93})$	A_1	$31x^2+3y^2$	$+1,-1,-1$
			$(2,1+\sqrt{-93})$	A	$47x^2+2xy+2y^2$	$-1,+1,-1$
-94	$\sqrt{-94}$	$-2^2\cdot 47$	(1)	J^8	$94x^2+y^2$	$+1,+1$
			$(5,4+\sqrt{-94})$	J^7	$22x^2+8xy+5y^2$	$-1,-1$
			$(7,5+\sqrt{-94})$	J^6	$17x^2+10xy+7y^2$	$+1,+1$
			$(11,4+\sqrt{-94})$	J^5	$10x^2+8xy+11y^2$	$-1,-1$
			$(2,\sqrt{-94})$	J^4	$47x^2+2y^2$	$+1,+1$
			$(11,7+\sqrt{-94})$	J^3	$13x^2+14xy+11y^2$	$-1,-1$
			$(7,2+\sqrt{-94})$	J^2	$14x^2+4xy+7y^2$	$+1,+1$
			$(5,1+\sqrt{-94})$	J	$19x^2+2xy+5y^2$	$-1,-1$
-95	$\frac{1}{2}(1+\sqrt{-95})$	$-5\cdot 19$	(1)	J^8	$24x^2+xy+y^2$	$+1,+1$

表 I (續)

D	ω	Δ	理想數	類	二次型	特徵系統
-95			$\left(2,\frac{1+\sqrt{-95}}{2}\right)$	J^7	$12x^2+xy+2y^2$	$-1,-1$
			$\left(4,\frac{1+\sqrt{-95}}{2}\right)$	J^6	$6x^2+xy+4y^2$	$+1,+1$
			$\left(3,\frac{5+\sqrt{-95}}{2}\right)$	J^5	$10x^2+5xy+3y^2$	$-1,-1$
			$\left(5,\frac{5+\sqrt{-95}}{2}\right)$	J^4	$6x^2+5xy+5y^2$	$+1,+1$
			$\left(3,\frac{1+\sqrt{-95}}{2}\right)$	J^3	$8x^2+xy+3y^2$	$-1,-1$
			$\left(4,\frac{7+\sqrt{-95}}{2}\right)$	J^2	$9x^2+7xy+4y^2$	$+1,+1$
			$\left(2,\frac{3+\sqrt{-95}}{2}\right)$	J	$13x^2+3xy+2y^2$	$-1,-1$
-97	$\sqrt{-97}$	$-2^2\cdot 97$	(1)	J^4	$97x^2+y^2$	$+1,+1$
			$(7,6+\sqrt{-97})$	J^3	$19x^2+12xy+7y^2$	$-1,-1$
			$(2,1+\sqrt{-97})$	J^2	$49x^2+2xy+2y^2$	$+1,+1$
			$(7,1+\sqrt{-97})$	J	$14x^2+2xy+7y^2$	$-1,-1$

表 II

D	ω	連分數表示	Δ	$x+y\sqrt{D}$	$N(x+y\sqrt{D})$	理想數	類	二次型	特徵系統
2	$\sqrt{2}$	$[1,\dot{2}]$	2^3	$1+\sqrt{2}$	-1	(1)	1	$-2x^2+y^2$	$+1$
3	$\sqrt{3}$	$[1,\dot{1},\dot{2}]$	$3\cdot2^2$	$2+\sqrt{3}$	$+1$	(1)	1	$-3x^2+y^2$	$+1, +1$
								$-x^2+3y^2$	$-1, -1$
5	$\frac{1}{2}(1+\sqrt{5})$	$[1,\dot{1}]$	5	ω	-1	(1)	1	$-x^2+xy+y^2$	$+1$
6	$\sqrt{6}$	$[2,\dot{2},\dot{4}]$	$3\cdot2^3$	$5+2\sqrt{6}$	$+1$	(1)	1	$-6x^2+y^2$	$+1, +1$
								$-x^2+6y^2$	$-1, -1$
7	$\sqrt{7}$	$[2,\dot{1},1,1,\dot{4}]$	$2^2\cdot7$	$8+3\sqrt{7}$	$+1$	(1)	1	$-7x^2+y^2$	$+1, +1$
								$-x^2+7y^2$	$-1, -1$
8		$[2,\dot{1},\dot{4}]$		$3+\sqrt{8}$	$+1$				
10	$\sqrt{10}$	$[3,\dot{6}]$	$5\cdot2^3$	$3+\sqrt{10}$	-1	(1)	A^2	$-10x^2+y^2$	$+1, +1$
						$(2,\sqrt{10})$	A	$-5x^2+2y^2$	$-1, -1$
11	$\sqrt{11}$	$[3,\dot{3},\dot{6}]$	$2^2\cdot11$	$10+3\sqrt{11}$	$+1$	(1)	1	$-11x^2+y^2$	$+1, +1$
								$-x^2+11y^2$	$-1, -1$
12		$[3,\dot{2},\dot{6}]$		$7+2\sqrt{12}$	$+1$				
13	$\frac{1}{2}(1+\sqrt{13})$	$[2,\dot{3}]$	13	$1+\omega$	-1	(1)	1	$-3x^2+xy+y^2$	$+1$
14	$\sqrt{14}$	$[3,\dot{1},2,1,\dot{6}]$	$7\cdot2^3$	$15+4\sqrt{14}$	$+1$	(1)	1	$-14x^2+y^2$	$+1, +1$
								$-x^2+14y^2$	$-1, -1$
15	$\sqrt{15}$	$[3,\dot{1},\dot{6}]$	$3\cdot2^2\cdot5$	$4+\sqrt{15}$	$+1$	(1)	A^2	$-15x^2+y^2$	$+1, +1, +1$
								$-x^2+15y^2$	$-1, +1, -1$

						$(2,1+\sqrt{15})$	A	$-7x^2+2xy+2y^2$	$-1,-1,+1$
								$-2x^2-2xy+7y^2$	$+1,-1,-1$
17	$\frac{1}{2}(1+\sqrt{17})$	$[2,\dot{1},1,\dot{3}]$	17	$3+2\omega$	-1	(1)	1	$-4x^2+xy+y^2$	$+1$
18		$[4,\dot{4},\dot{8}]$		$17+4\sqrt{18}$	$+1$				
19	$\sqrt{19}$	$[4,\dot{2},1,3,1,2,\dot{8}]$	$2^2\cdot19$	$170+39\sqrt{19}$	$+1$	(1)	1	$-19x^2+y^2$	$+1,+1$
								$-x^2+19y^2$	$-1,-1$
20		$[4,\dot{2},\dot{8}]$		$9+2\sqrt{20}$	$+1$				
21	$\frac{1}{2}(1+\sqrt{21})$	$[2,\dot{1},\dot{3}]$	$3\cdot7$	$2+\omega$	$+1$	(1)	1	$-5x^2+xy+y^2$	$+1,+1$
								$-x^2-xy+5y^2$	$-1,-1$
22	$\sqrt{22}$	$[4,\dot{1},2,4,2,1,\dot{8}]$	$2^2\cdot11$	$197+42\sqrt{22}$	$+1$	(1)	1	$-22x^2+y^2$	$+1,+1$
								$-x^2+22y^2$	$-1,-1$
23	$\sqrt{23}$	$[4,\dot{1},3,1,\dot{8}]$	$2^2\cdot23$	$24+5\sqrt{27}$	$+1$	(1)	1	$-23x^2+y^2$	$+1,+1$
								$-x^2+23y^2$	$-1,-1$
24		$[4,\dot{1},\dot{8}]$		$5+\sqrt{24}$	$+1$				
26	$\sqrt{26}$	$[5,\dot{10}]$	$2^3\cdot13$	$5+\sqrt{26}$	-1	(1)	A^2	$-26x^2+y^2$	$+1,+1$
						$(2,\sqrt{26})$	A	$-13x^2+2y^2$	$-1,-1$
27		$[5,\dot{5},\dot{10}]$		$26+5\sqrt{27}$	$+1$				
28		$[5,\dot{3},2,3,\dot{10}]$		$127+24\sqrt{28}$	$+1$				
29	$\frac{1}{2}(1+\sqrt{29})$	$[3,\dot{5}]$	29	$2+\omega$	-1	(1)	1	$-7x^2+xy+y^2$	$+1$

表 II (續)

D	ω	連分數表示	Δ	$x+y\sqrt{D}$	$N(x+y\sqrt{D})$	理想數	類	二次型	特徵系統
30	$\sqrt{30}$	$[5,\dot{2},\dot{10}]$	$3\cdot5\cdot2^3$	$11+2\sqrt{30}$	$+1$	(1)	A^2	$-30x^2+y^2$	$+1,+1,+1$
								$-x^2+30y^2$	$-1,+1,-1$
						$(2,\sqrt{30})$	A	$-15x^2+2y^2$	$-1,-1,+1$
								$-2x^2+15y^2$	$+1,-1,-1$
31	$\sqrt{31}$	$[5,\dot{1},1,3,5,3,1,1,\dot{10}]$	$2^2\cdot31$	$1520+273\sqrt{31}$	$+1$	(1)	1	$-31x^2+y^2$	$+1,+1$
								$-x^2+31y^2$	$-1,-1$
32		$[5,\dot{1},1,1,\dot{10}]$		$17+3\sqrt{32}$	$+1$				
33	$\frac{1}{2}(1+\sqrt{33})$	$[3,\dot{2},1,2,\dot{5}]$	$3\cdot11$	$19+8\omega$	$+1$	(1)	1	$-8x^2+xy+y^2$	$+1,+1$
								$-x^2-xy+8y^2$	$-1,-1$
34	$\sqrt{34}$	$[5,\dot{1},4,1,\dot{10}]$	$2^3\cdot17$	$35+6\sqrt{34}$	$+1$	(1)	A^2	$-34x^2+y^2$	$+1,+1$
								$-x^2+34y^2$	$+1,+1$
						$(3,1+\sqrt{34})$	A	$-11x^2+2xy+3y^2$	$-1,-1$
								$-3x^2-2xy+11y^2$	$-1,-1$
35	$\sqrt{35}$	$[5,\dot{1},\dot{10}]$	$2^2\cdot5\cdot7$	$6+\sqrt{35}$	$+1$	(1)	A^2	$-35x^2+y^2$	$+1,+1,+1$
								$-x^2+35y^2$	$+1,-1,-1$
						$(2,1+\sqrt{35})$	A	$-17x^2+2xy+2y^2$	$-1,+1,-1$
								$-2x^2-2xy+17y^2$	$-1,-1,+1$
37	$\frac{1}{2}(1+\sqrt{37})$	$[3,\dot{1},1,\dot{5}]$	37	$5+2\omega$	-1	(1)	1	$-9x^2+xy+y^2$	$+1$
38	$\sqrt{38}$	$[6,\dot{6},\dot{12}]$	$2^3\cdot19$	$37+6\sqrt{38}$	$+1$	(1)	1	$-38x^2+y^2$	$+1,+1$

								$-x^2+38y^2$	$-1,-1$
39	$\sqrt{39}$	$[6,\dot{4},\dot{12}]$	$3\cdot2^2\cdot13$	$25+4\sqrt{39}$	$+1$	(1)	A^2	$-39x^2+y^2$	$+1,+1,+1$
								$-x^2+39y^2$	$-1,+1,-1$
						$(2,1+\sqrt{39})$	A	$-19x^2+2xy+2y^2$	$-1,-1,+1$
								$-2x^2-2xy+19y^2$	$+1,-1,-1$
40		$[6,\dot{3},\dot{12}]$		$19+3\sqrt{40}$	$+1$				
41	$\frac{1}{2}(1+\sqrt{41})$	$[3,\dot{1},2,2,1,\dot{5}]$	41	$27+10\omega$	-1	(1)	1	$-10x^2+xy+y^2$	$+1$
42	$\sqrt{42}$	$[6,\dot{2},\dot{12}]$	$3\cdot2^3\cdot7$	$13+2\sqrt{42}$	$+1$	(1)	A^2	$-42x^2+y^2$	$+1,+1,+1$
								$-x^2+42y^2$	$-1,-1,+1$
						$(2,\sqrt{42})$	A	$-21x^2+2y^2$	$-1,+1,-1$
								$-2x^2+21y^2$	$+1,-1,-1$
43	$\sqrt{43}$	$[6,\dot{1},1,3,1,5,1,3,1,1,\dot{12}]$	$2^2\cdot43$	$3482+531\sqrt{43}$	$+1$	(1)	1	$-43x^2+y^2$	$+1,+1$
								$-x^2+43y^2$	$-1,-1$
44		$[6,\dot{1},1,1,2,1,1,1,\dot{12}]$		$199+30\sqrt{44}$	$+1$				
45		$[6,\dot{1},2,2,2,1,\dot{12}]$		$161+24\sqrt{45}$	$+1$				
46	$\sqrt{46}$	$[6,\dot{1},3,1,1,2,6,2,1,1,3,1,\dot{12}]$	$2^3\cdot23$	$24335+3588\sqrt{46}$	$+1$	(1)	1	$-46x^2+y^2$	$+1,+1$
								$-x^2+46y^2$	$-1,-1$
47	$\sqrt{47}$	$[6,\dot{1},5,1,\dot{12}]$	$2^2\cdot47$	$48+7\sqrt{47}$	$+1$	(1)	1	$-47x^2+y^2$	$+1,+1$
								$-x^2+47y^2$	$-1,-1$

表 II (續)

D	ω	連分數表示	Δ	$x+y\sqrt{D}$	$N(x+y\sqrt{D})$	理想數	類	二次型	特徵系統
48		$[6,\dot{1},\dot{12}]$		$7+\sqrt{49}$	$+1$				
50		$[7,\dot{14}]$		$7+\sqrt{50}$	-1				
51	$\sqrt{51}$	$[7,\dot{7},\dot{14}]$	$3\cdot2^2\cdot17$	$50+7\sqrt{51}$	$+1$	(1)	A^2	$-51x^2+y^2$	$+1,+1,+1$
								$-x^2+51y^2$	$-1,+1,-1$
						$(3,\sqrt{51})$	A	$-17x^2+3y^2$	$+1,-1,-1$
								$-3x^2+17y^2$	$-1,-1,+1$
52		$[7,\dot{4},1,2,1,4,\dot{14}]$		$649+90\sqrt{52}$	$+1$				
53	$\frac{1}{2}(1+\sqrt{53})$	$[4,\dot{7}]$	53	$3+\omega$	-1	(1)	1	$-13x^2+xy+y^2$	$+1$
54		$[7,\dot{2},1,6,1,2,\dot{14}]$		$485+66\sqrt{54}$	$+1$				
55	$\sqrt{55}$	$[7,\dot{2},2,2,\dot{14}]$	$2^2\cdot5\cdot11$	$89+12\sqrt{55}$	$+1$	(1)	A^2	$-55x^2+y^2$	$+1,+1,+1$
								$-x^2+55y^2$	$+1,-1,-1$
						$(2,1+\sqrt{55})$	A	$-27x^2+2xy+2y^2$	$-1,-1,+1$
								$-2x^2-2xy+27y^2$	$-1,+1,-1$
56		$[7,\dot{2},\dot{14}]$		$15+2\sqrt{56}$	$+1$				
57	$\frac{1}{2}(1+\sqrt{57})$	$[4,\dot{3},1,1,1,3,\dot{7}]$	$3\cdot19$	$131+40\omega$	$+1$	(1)	1	$-14x^2+xy+y^2$	$+1,+1$
								$-x^2-xy+14y^2$	$-1,-1$
58	$\sqrt{58}$	$[7,\dot{1},1,1,1,1,1,\dot{14}]$	$2^3\cdot29$	$99+13\sqrt{58}$	-1	(1)	A^2	$-58x^2+y^2$	$+1,+1$
						$(2,\sqrt{58})$	A	$-29x^2+2y^2$	$-1,-1$
59	$\sqrt{59}$	$[7,\dot{1},2,7,2,1,\dot{14}]$	$2^2\cdot59$	$530+69\sqrt{59}$	$+1$	(1)	1	$-59x^2+y^2$	$+1,+1$

								$-x^2+59y^2$	$-1,-1$
60		$[7,\dot{1},2,1,\dot{14}]$		$31+4\sqrt{60}$	$+1$				
61	$\frac{1}{2}(1+\sqrt{61})$	$[4,\dot{2},2,\dot{7}]$	61	$17+5\omega$	-1	(1)	1	$-15x^2+xy+y^2$	$+1$
62	$\sqrt{62}$	$[7,\dot{1},6,1,\dot{14}]$	$2^2\cdot 31$	$63+8\sqrt{62}$	$+1$	(1)	1	$-62x^2+y^2$	$+1,+1$
								$-x^2+62y^2$	$-1,-1$
63		$[7,\dot{1},\dot{14}]$		$8+\sqrt{64}$	$+1$				
65	$\frac{1}{2}(1+\sqrt{65})$	$[4,\dot{1},1,\dot{7}]$	$5\cdot 13$	$7+2\omega$	-1	(1)	A^2	$-16x^2+xy+y^2$	$+1,+1$
						$\left(5,2+\frac{1+\sqrt{65}}{2}\right)$	A	$-2x^2+5xy+5y^2$	$-1,-1$
66	$\sqrt{66}$	$[8,\dot{8},\dot{16}]$	$3\cdot 2^2\cdot 11$	$65+8\sqrt{66}$	$+1$	(1)	A^2	$-66x^2+y^2$	$+1,+1,+1$
								$-x^2+66y^2$	$-1,-1,+1$
						$(3,\sqrt{66})$	A	$-22x^2+3y^2$	$-1,+1,-1$
								$-3x^2+22y^2$	$+1,-1,-1$
67	$\sqrt{67}$	$[8,\dot{5},2,1,1,7,1,1,2,5,\dot{16}]$	$2^2\cdot 67$	$48842+5967\sqrt{67}$	$+1$	(1)	1	$-67x^2+y^2$	$+1,+1$
								$-x^2+67y^2$	$-1,-1$
68		$[8,\dot{4},\dot{16}]$		$33+4\sqrt{68}$	$+1$				
69	$\frac{1}{2}(1+\sqrt{69})$	$[4,\dot{1},1,1,\dot{7}]$	$3\cdot 23$	$11+3\omega$	$+1$	(1)	1	$-17x^2+xy+y^2$	$+1,+1$
								$-x^2-xy+17y^2$	$-1,-1$
70	$\sqrt{70}$	$[8,\dot{2},1,2,1,2,\dot{16}]$	$5\cdot 7\cdot 2^3$	$251+30\sqrt{70}$	$+1$	(1)	A^2	$-70x^2+y^2$	$+1,+1,+1$
								$-x^2+70y^2$	$+1,-1,-1$

表 II (續)

D	ω	連分數表示	Δ	$x+y\sqrt{D}$	$N(x+y\sqrt{D})$	理想數	類	二次型	特徵系統
70						$(2,\sqrt{70})$	A	$-35x^2+2y^2$	$-1,+1,-1$
								$-2x^2+35y^2$	$-1,-1,+1$
71	$\sqrt{71}$	$[8,\dot{2},2,1,7,1,2,2,\dot{16}]$	$2^2\cdot71$	$3480+413\sqrt{71}$	$+1$	(1)	1	$-71x^2+y^2$	$+1,+1$
								$-x^2+71y^2$	$-1,-1$
72		$[8,\dot{2},\dot{16}]$		$17+2\sqrt{72}$	$+1$				
73	$\frac{1}{2}(1+\sqrt{73})$	$[4,1,3,2,1,1,2,3,1,\dot{7}]$	73	$943+250\omega$	-1	(1)	1	$-18x^2+xy+y^2$	$+1$
74	$\sqrt{74}$	$[8,\dot{1},1,1,1,\dot{16}]$	$2^3\cdot37$	$43+5\sqrt{74}$	-1	(1)	A^2	$-74x^2+y^2$	$+1,+1$
						$(2,\sqrt{74})$	A	$-37x^2+2y^2$	$-1,-1$
75		$[8,\dot{1},1,1,\dot{16}]$		$26+3\sqrt{75}$	$+1$				
76		$[8,\dot{1},2,1,1,5.4,5,1,1,2,1,\dot{16}]$		$57799+6630\sqrt{76}$	$+1$				
77	$\frac{1}{2}(1+\sqrt{77})$	$[4,\dot{1},\dot{7}]$	$7\cdot11$	$4+\omega$	$+1$	(1)	1	$-19x^2+xy+y^2$	$+1,+1$
								$-x^2-xy+19y^2$	$-1,-1$
78	$\sqrt{78}$	$[8,\dot{1},4,1,\dot{16}]$	$3\cdot2^3\cdot13$	$53+6\sqrt{78}$	$+1$	(1)	A^2	$-78x^2+y^2$	$+1,+1,+1$
								$-x^2+78y^2$	$-1,+1,-1$
						$(2,\sqrt{78})$	A	$-39x^2+2y^2$	$-1,-1,+1$
								$-2x^2+39y^2$	$+1,-1,-1$
79	$\sqrt{79}$	$[8,\dot{1},7,1,\dot{16}]$	$2^2\cdot79$	$80+9\sqrt{79}$	$+1$	(1)	I^3	$-79x^2+y^2$	$+1,+1$
								$-x^2+79y^2$	$-1,-1$
						$(3,2+\sqrt{79})$	I^2	$-25x^2+4xy+3y^2$	$-1,-1$

								$-3x^2-4xy+25y^2$	$+1, +1$
						$(3,1+\sqrt{79})$	I	$-26x^2+2xy+3y^2$	$-1, -1$
								$-3x^2-2xy+26y^2$	$+1, +1$
80		$[8,\dot{1},\dot{16}]$		$9+\sqrt{80}$	$+1$				
82	$\sqrt{82}$	$[9,\dot{1}\dot{8}]$	$2^3\cdot 41$	$9+\sqrt{82}$	-1	(1)	I^4	$-82x^2+y^2$	$+1, +1$
						$(3,1+\sqrt{82})$	I^3	$-27x^2+2xy+3y^2$	$-1, -1$
						$(2,\sqrt{82})$	I^2	$-41x^2+2y^2$	$+1, +1$
						$(3,2+\sqrt{82})$	I	$-26x^2+4xy+3y^2$	$-1, -1$
83	$\sqrt{83}$	$[9,\dot{9},\dot{18}]$	$2^2\cdot 83$	$82+9\sqrt{83}$	$+1$	(1)	1	$-83x^2+y^2$	$+1, +1$
								$-x^2+83y^2$	$-1, -1$
84		$[9,\dot{6},\dot{18}]$		$55+6\sqrt{84}$	$+1$				
85	$\frac{1}{2}(1+\sqrt{85})$	$[5,\dot{9}]$	$5\cdot 17$	$4+\omega$	-1	(1)	A^2	$-21x^2+xy+y^2$	$+1, +1$
						$\left(5, 2+\frac{1+\sqrt{85}}{2}\right)$	A	$-3x^2+5xy+5y^2$	$-1, -1$
86	$\sqrt{86}$	$[9,\dot{3},1,1,1,8,1,1,1,3,\dot{18}]$	$2^3\cdot 43$	$10405+1122\sqrt{86}$	$+1$	(1)	1	$-86x^2+y^2$	$+1, +1$
								$-x^2+86y^2$	$-1, -1$
87	$\sqrt{87}$	$[9,\dot{3},\dot{18}]$	$3\cdot 2^2\cdot 29$	$28+3\sqrt{87}$	$+1$	(1)	A^2	$-87x^2+y^2$	$+1, +1, +1$
								$-x^2+87y^2$	$-1, +1, -1$
						$(2,1+\sqrt{87})$	A	$-43x^2+2xy+2y^2$	$-1, -1, +1$
								$-2x^2-2xy+43y^2$	$+1, -1, -1$

表 II (續)

D	ω	連分數表示	Δ	$x+y\sqrt{D}$	$N(x+y\sqrt{D})$	理想數	類	二次型	特徵系統
88		$[9,\dot{2},1,1,1,2,\dot{18}]$		$197+21\sqrt{88}$	$+1$				
89	$\frac{1}{2}(1+\sqrt{89})$	$[5,\dot{4},1,1,1,1,4,\dot{9}]$	89	$447+106\omega$	-1	(1)	1	$-22x^2+xy+y^2$	$+1$
90		$[9,\dot{2},\dot{18}]$		$19+2\sqrt{90}$	$+1$				
91	$\sqrt{91}$	$[9,\dot{1},1,5,1,5,1,1,\dot{18}]$	$2^2\cdot7\cdot13$	$1574+165\sqrt{91}$	$+1$	(1)	A^2	$-91x^2+y^2$	$+1,+1,+1$
								$-x^2+91y^2$	$-1,+1,-1$
						$(2,1+\sqrt{91})$	A	$-45x^2+2xy+2y^2$	$+1,-1,-1$
								$-2x^2-2xy+45y^2$	$-1,-1,+1$
92		$[9,\dot{1},1,2,4,2,1,1,\dot{18}]$		$1151+120\sqrt{92}$	$+1$				
93	$\frac{1}{2}(1+\sqrt{93})$	$[5,\dot{3},\dot{9}]$	$3\cdot31$	$13+3\omega$	$+1$	(1)	1	$-23x^2+xy+y^2$	$+1,+1$
								$-x^2-xy+23y^2$	$-1,-1$
94	$\sqrt{94}$	$[9,\dot{1},2,3,1,1,5,1,8,1,5,$ $1,1,3,2,1,\dot{18}]$	$2^3\cdot47$	$2143295+221064\sqrt{94}$	$+1$	(1)	1	$-94x^2+y^2$	$+1,+1$
								$-x^2+94y^2$	$-1,-1$
95	$\sqrt{95}$	$[9,\dot{1},2,1,\dot{18}]$	$2^2\cdot5\cdot19$	$39+4\sqrt{95}$	$+1$	(1)	A^2	$-95x^2+y^2$	$+1,+1,+1$
								$-x^2+95y^2$	$+1,-1,-1$
						$(2,1+\sqrt{95})$	A	$-47x^2+2xy+2y^2$	$-1,-1,+1$
								$-2x^2-2xy+47y^2$	$-1,+1,-1$
96		$[9,\dot{1},3,1,\dot{18}]$		$49+5\sqrt{96}$	$+1$				
97	$\frac{1}{2}(1+\sqrt{97})$	$[5,\dot{2},2,1,4,4,1,2,2,\dot{9}]$	97	$5035+1138\omega$	-1	(1)	1	$-24x^2+xy+y^2$	$+1$
98		$[9,\dot{1},8,1,\dot{18}]$		$99+10\sqrt{98}$	$+1$				
99		$[9,\dot{1},\dot{18}]$		$10+\sqrt{99}$	$+1$				

第 十 七 章

代數數與超越數

§1. 超越數之存在定理.

一實數可以視爲直線上之一點. 一組實數稱爲一個點集. 例如: $\left\{\frac{1}{n}\right\}$, $n=1,2,\cdots$成一點集. 所有的有理數成一點集. 所有a,b之間的實數也成一點集.

定義 1. 如果兩點集之點間可以建立一個一對一的對應關係,則此二點集謂之同冪. 卽二點集 A 及 B 中,對應於 A 之任一點, B 中有唯一點與之對應,且其逆亦然. 同冪之關係有次之三性質: (i) A 與 A 同冪; (ii) 若 A 與 B 同冪,則 B 與 A 同冪; (iii) 若 A 與 B, B 與 C 同冪,則 A 與 C 同冪.

例 1. $\left\{\frac{1}{n}\right\}$, $n=1,2,3,\cdots$ 所成之點集與自然數集同冪.

例 2. 適合於 $0\leqslant x\leqslant 1$ 之實數 x 所成之集與適合於 $1\leqslant y\leqslant 2$ 之實數 y 所成之集同冪.

定義 2. 凡與自然數集同冪之集謂之無限可數集. 無限可數集與有限集皆稱爲可數集.

故自然數集是可數集. $\left\{\frac{1}{n}\right\}$, $n=1,2,3,\cdots$ 是可數集. 任一貫是一可數集.

定理 1. 可數個可數集之總集仍爲可數集.

證: 命 $M_1,M_2,\cdots$ 爲可數個可數集. 更命

$$M_i=(a_{i1},\cdots,a_{ij},\cdots).$$

總集是

$$\begin{array}{cccc}
a_{11} & a_{12} & a_{13} & a_{14}\cdots \\
\swarrow & \swarrow & & \\
a_{21} & a_{22} & \cdots & \\
\swarrow & & & \\
a_{31} & \cdots & & \\
\cdots\cdots\cdots\cdots & & &
\end{array}$$

依箭向排列：

$$\alpha_{11},\ \alpha_{12},\ \alpha_{21},\ \alpha_{13},\ \alpha_{22},\ \alpha_{31},\ \alpha_{14},\ \cdots.$$

故得定理.

定 理 2. 有理數集是可數集.

證： 由定理 1 可知,吾人祇需證明：0 與 1 之間的有理數成一可數集卽足. 將 0 與 1 之間的既約分數先依分母之大小,再依分子之大小排列之,則得

$$\frac{0}{1},\ \frac{1}{1},\ \frac{1}{2},\ \frac{1}{3},\ \frac{2}{3},\ \frac{1}{4},\ \frac{3}{4},\ \frac{1}{5},\ \frac{2}{5},\ \frac{3}{5},\ \frac{4}{5},\ \cdots.$$

故得定理.

定 理 3. $(0,1)$ 之間諸實數所成之集爲不可數集.

證： 若定理不成立,則可設 $(0,1)$ 之間諸實數已排成

$$\alpha_1,\ \alpha_2,\ \alpha_3,\ \cdots$$

之形. 以小數表此諸數,則得

$$\alpha_i = 0.\, a_{i1}\, a_{i2} \cdots a_{in} \cdots, \qquad 0 \leqslant a_{in} \leqslant 9.$$

作一數

$$\beta = 0.\, b_1\, b_2 \cdots b_n \cdots,$$

此處

$$b_i = \begin{cases} a_{ii} + 1, & \text{若}\quad 0 \leqslant a_{ii} \leqslant 5; \\ a_{ii} - 1, & \text{若}\quad 6 \leqslant a_{ii} \leqslant 9. \end{cases}$$

β 是 $(0,1)$ 之間的一實數,但並不等於任一 α_i, 因爲其中第 i 位小數不同. 此乃一矛盾. (並須注意：在小數表示法中

$$0.12 = 0.11999\cdots,$$

而現在 β 之小數中 9 及 0 並不出現.)

習題 1. 求出定理 2 之證明中 $\frac{a}{b}$ $((a,b)=1)$ 之地位.

習題 2. 證明可數集之分集爲可數集.

前章已定義：一代數數 ξ 乃適合方程

$$a_n \xi^n + a_{n-1} \xi^{n-1} + \cdots + a_0 = 0$$

之根,此處 $a_n, a_{n-1}, \cdots, a_0$ 是有理整數. 若此式不可分解, 且 $a_n \neq 0$, 則此 ξ 稱爲 n 次的代數數. 若 $a_n = 1$, 則此 ξ 稱爲 n 次的代數整數.

定 理 4. 諸代數數所成之集是可數的.

證：命

$$N = n + |a_n| + |a_{n-1}| + \cdots + |a_0|.$$

顯然 $N \geqslant 2$. 對同一 N, 僅有有限個多項式. 每一個多項式的根數也有限. 故有同一 N 的代數數是有限的. 此諸代數數所成之集以 E_N 表之. 今列出

$$E_2, E_3, \cdots, E_N, \cdots.$$

命 E'_N 表 E_N 中之數而不在 $E_2, \cdots, E_{N-1}$ 之中者所成之集. 如此,則得

$$E_2, E'_3, \cdots, E'_N, \cdots$$

爲可數個有限集. 由定理 1 可知其總集爲可數集. 定理已明.

定義 3. 非代數數之數稱爲超越數.

定理 5. 有超越數存在.

證：由定理 3 及習題 2, 已知所有的實數成一不可數集,而實代數數乃一可數集,故得定理.

§ 2. Liouville 定理及超越數例子.

定理 1 (Liouville). 任一 n 次實代數數不能有 n 級以上之有理漸近分數. 即若 是一 n 次代數數,則對任一 $\varepsilon > 0$ 及 $A > 0$, 不等式

$$\left|\xi - \frac{p}{q}\right| < \frac{A}{q^{n+\varepsilon}} \tag{1}$$

之有理整數解 (p, q) 的對數有限.

證：設 ξ 適合於

$$f(\xi) = a_n \xi^n + a_{n-1} \xi^{n-1} + \cdots + a_0 = 0.$$

顯然有一數 $M = M(\xi)$ 存在,使當 y 在 $\xi - 1 < y < \xi + 1$ 中變化時

$$|f'(y)| < M.$$

若有有理數 $\frac{p}{q}$ $(q > 0)$ 與 ξ 接近, 可設 $\xi - 1 < \frac{p}{q} < \xi + 1$ 及 $f\left(\frac{p}{q}\right) \neq 0$, 如是顯然有

$$\left|f\left(\frac{p}{q}\right)\right| = \frac{|a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_0 q^n|}{q^n} \geqslant \frac{1}{q^n},$$

又

$$f\left(\frac{p}{q}\right) = f\left(\frac{p}{q}\right) - f(\xi) = \left(\frac{p}{q} - \xi\right) f'(\eta),$$

此 η 在 $\frac{p}{q}$ 與 ξ 之間. 故

$$\left|\xi-\frac{p}{q}\right|=\frac{\left|f\left(\frac{p}{q}\right)\right|}{|f'(\eta)|}>\frac{1}{M\,q^{n}}.$$

故對任一 $\varepsilon>0$ 及 $A>0$, (1) 式的有理整數解 (p, q) 的對數有限.

今舉出兩個作超越數之方法:

定理 2.

$$\xi=\frac{1}{10}+\frac{1}{10^{2!}}+\frac{1}{10^{3!}}+\cdots$$

及

$$\xi=\frac{1}{10}+\frac{1}{10^{2!}}+\frac{1}{10^{3!}}+\cdots$$

皆爲超越數.

證: 1) 命

$$\alpha_n=\frac{1}{10}+\frac{1}{10^{2!}}+\cdots+\frac{1}{10^{n!}}=\frac{p}{q}, \qquad q=10^{n!}$$

則

$$0<\xi-\frac{p}{q}=\frac{1}{10^{(n+1)!}}+\cdots<$$

$$<\frac{2}{10^{(n+1)!}}=\frac{2}{q^{n+1}},$$

此 n 可以任意,故由定理 1 可知 ξ 不是代數數.

2) 命

$$\xi=\frac{1}{10}+\frac{1}{10^{2!}}+\frac{1}{10^{3!}}+\cdots=[0, a_1, a_2, a_3, \cdots],$$

又命 p_n/q_n 爲其第 n 個漸近值,則

$$\left|\xi-\frac{p_n}{q_n}\right|<\frac{1}{q_n\,q_{n+1}}<\frac{1}{a_{n+1}\,q_n^2}<\frac{1}{a_{n+1}}.$$

現在 $a_{n+1}=10^{(n+1)!}$, 且

$$q_1<a_1+1, \quad \frac{q_{n+1}}{q_n}=a_{n+1}+\frac{q_{n-1}}{q_n}<a_{n+1}+1 \qquad (n\geqslant 1),$$

故

$$q_n<(a_1+1)(a_2+1)\cdots(a_n+1)<$$

$$<\left(1+\frac{1}{10}\right)\left(1+\frac{1}{10^2}\right)\cdots\left(1+\frac{1}{10^n}\right)a_1 a_2 \cdots a_n <$$

$$< 2\,a_1 a_2 \cdots a_n = 2\cdot 10^{1!+2!+\cdots+n!} < 10^{2\cdot n!} = a_n^2.$$

因此

$$\left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{a_{n+1}} = \frac{1}{a_n^{n+1}} < \frac{1}{a_n^n} < \frac{1}{q_n^{\frac{1}{2}n}},$$

如 1),可知 ξ 乃超越數.

習題. 作出一不可數集,其中每一數都是超越數.

提示 命 $a_1 \leqslant a_2 \leqslant a_3 \leqslant \cdots$ 爲一遞增自然數貫,則

$$\frac{1}{10^{a_1}} + \frac{1}{10^{a_2\cdot 2!}} + \frac{1}{10^{a_3\cdot 3!}} + \cdots$$

是一超越數.

§3. 代數數的有理逼近定理.

本節之目的在於將定理 2.1 更精密化. 命 κ 爲最小正數,使對任與之 n ($\geqslant 2$) 次代數數 α, 當 $\nu > \kappa$ 時,不等式

$$\left|\alpha - \frac{h}{q}\right| < \frac{1}{q^\nu}$$

僅有有限對有理整數解 h, q. 由定理 2.1 已知 $\kappa \leqslant n$. Thue 證明了 $\kappa \leqslant \frac{1}{2}n + 1$. Siegel 證明 $\kappa \leqslant \min\limits_{1\leqslant s\leqslant n-1}\left(s + \frac{n}{s+1}\right)$. Dyson 證明 $\kappa \leqslant \sqrt{2n}$. 直至最近 (1955 年), 此問題才爲 Roth 所解決. 彼證明 $\kappa \leqslant 2$. 此結果爲至善者,因爲對任一無理數 α 常有無限對 (h, q) 使

$$\left|\alpha - \frac{h}{q}\right| \leqslant \frac{1}{q^2}.$$

定理 1 (Roth). 命 α 爲任一非有理數之代數數. 若有無限多對有理整數 (h, q) 使

$$\left|\alpha - \frac{h}{q}\right| < \frac{1}{q^\kappa},$$

則 $\kappa \leqslant 2$.

此定理之證明較爲複雜,初學者可以從略.

1. 我們先述次之諸引.

引 1. 命

$$D = \begin{vmatrix} a_{11} \cdots a_{1m} \\ \cdots\cdots\cdots\cdots \\ a_{m1} \cdots a_{mm} \end{vmatrix} \neq 0, \quad E = \begin{vmatrix} a_{11} & \cdots & a_{1m} & c_1 \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mm} & c_m \\ b_1 & \cdots & b_m & c \end{vmatrix} = 0,$$

則方程組

$$\sum_{\lambda=1}^{m} a_{\kappa\lambda} y_\lambda = c_\kappa \qquad (\kappa = 1, \cdots, m)$$

之解 $y_1, \cdots, y_m$ 恆適合於

$$\sum_{\lambda=1}^{m} b_\lambda y_\lambda = c.$$

此乃行列式論中一習知的定理,證從略.

定義 1. $f_1(x), \cdots, f_m(x)$ 是 m 個具有有理係數的多項式. 若有一組不全爲零之有理數 $c_1, \cdots, c_m$, 使

$$\sum_{\lambda=1}^{m} c_\lambda f_\lambda(x) \equiv 0,$$

則此 m 個多項式稱爲互依,不然,則稱爲非互依或獨立.

引 2. 若行列式

$$E = \left| \frac{1}{\kappa!} f_\lambda^{(\kappa)}(x) \right| \qquad (\kappa = 0, \cdots, m-1;\ \lambda = 1, \cdots, m)$$

恆等於 0, 則 $f_1(x), \cdots, f_m(x)$ 互依, 此處 $f_\lambda^{(\kappa)}(x)$ 表 $f_\lambda(x)$ 之 κ 次導數. 行列式 E 稱爲 $f_1, \cdots, f_m$ 之 Wronskian.

證: $m = 1$ 時定理顯然成立. 今於 m 上行歸納法. 假定定理對 $m-1$ 已眞實. 若 $f_1(x), \cdots, f_{m-1}(x)$ 互依, 則 $f_1(x), \cdots, f_m(x)$ 顯然互依. 故可假定 $f_1(x), \cdots, f_{m-1}(x)$ 非互依. 由歸納法假定,可知

$$D = | f_\lambda^{(\kappa)}(x) | \qquad (\kappa = 0, \cdots, m-2;\ \lambda = 1, \cdots, m-1)$$

不恆爲 0. 故必存在一區間 $a < x < b$, 使得 D 在其中恆不爲 0. 由引 1, 已知適合於

$$\sum_{\lambda=1}^{m-1} f_\lambda^{(\kappa)}(x)\, y_\lambda = f_m^{(\kappa)}(x) \qquad (\kappa = 0, \cdots, m-2) \tag{1}$$

之解必適合

$$\sum_{\lambda=1}^{m-1} f_\lambda^{(m-1)}(x)\, y_\lambda = f_m^{(m-1)}(x). \tag{2}$$

微分 (1) 式,可得

$$\sum_{\lambda=1}^{m-1} f_\lambda^{(\kappa+1)}(x)\, y_\lambda + \sum_{\lambda=1}^{m-1} f_\lambda^{(\kappa)}(x)\, y'_\lambda = f_m^{(\kappa+1)}(x) \qquad (\kappa = 0, \cdots, m-2).$$

再由 (1) 及 (2), 可知

$$\sum_{\lambda=1}^{m-1} f_\lambda^{(\kappa)}(x)\, y'_\lambda = 0 \qquad (\kappa = 0, \cdots, m-2).$$

因 D 在 $a < x < b$ 中恆不爲 0, 故得

$$y'_1 = \cdots = y'_{m-1} = 0.$$

卽

$$y_\lambda = c_\lambda, \quad (\lambda = 1, \cdots, m-1),$$

於此, c_λ 是常數. 又因 y_λ 是 x 之有理函數,其係數爲有理數, 故 c_λ 爲有理數. 由 (1) 可知

$$\sum_{\lambda=1}^{m-1} c_\lambda f_\lambda(x) = f_m(x)$$

在 $a < x < b$ 中成立. 因 $f_\lambda(x)$ 是多項式,故此式恆成立. 引理卽已證明.

記微分運算

$$\Delta = \frac{1}{i_1! \cdots i_p!} \left(\frac{\partial}{\partial x_1}\right)^{i_1} \cdots \left(\frac{\partial}{\partial x_p}\right)^{i_p}, \tag{3}$$

並稱 $i_1 + \cdots + i_p$ 爲 Δ 之階, 我們現將 Wronskian 推廣到多個變數的多項式之情況.

定義 2. 設

$$\varphi_0(x_1, \cdots, x_p), \cdots, \varphi_{l-1}(x_1, \cdots, x_p)$$

爲 p 個變數 $x_1, \cdots, x_p$ 之多項式, $\Delta_0, \Delta_1, \cdots, \Delta_{l-1}$ 爲 l 個形如 (3) 之微分運算,其各之階分別至多爲 $0, 1, \cdots, l-1$. 則行列式

$$G(x_1, \cdots, x_p) = |\, \Delta_\mu\, \varphi_\nu(x_1, \cdots, x_p)\, | \quad (\mu, \nu = 0, \cdots, l-1)$$

稱爲 $\varphi_0, \cdots, \varphi_{l-1}$ 之廣義 Wronskian.

顯而易見,若 $p > 1$, $l > 1$, 則此種廣義 Wronskian 不祇一個,但這並不會使我們下面的推理發生曖昧.

引 3. 設 $\varphi_0(x_1, \cdots, x_p), \cdots, \varphi_{l-1}(x_1, \cdots, x_p)$ 爲 l 個線性獨立之多項式,其係數爲有理數,則其廣義 Wronskian 中,至少有一個不恆爲 0.

證: 設 k 爲一整數,它大於諸多項式 $\varphi_0, \cdots, \varphi_{l-1}$ 中各變數 $x_1, \cdots, x_p$ 的所有指數. 則 l 個多項式

$$\varphi_\nu(t,\ t^k,\ t^{k^2}, \cdots, t^{k^{p-1}}) \quad (\nu = 0, \cdots, l-1) \tag{4}$$

爲線性獨立. 蓋令

$$\varphi_\nu(x_1, \cdots, x_p) = \sum_{s_1=0}^{k-1} \cdots \sum_{s_p=0}^{k-1} b^{(\nu)}(s_1, \cdots, s_p)\, x_1^{s_1} \cdots x_p^{s_p},$$

若 (4) 爲線性互依,則必存在有理數 $c_0, \cdots, c_{l-1}$ 使

$$\sum_{\nu=0}^{l-1} c_\nu \sum_{s_1=0}^{k-1} \cdots \sum_{s_p=0}^{k-1} b^{(\nu)}(s_1, \cdots, s_p)\, t^{s_1 + ks_2 + \cdots + k^{p-1}s_p} \equiv 0\,. \tag{5}$$

因每一整數只能以一種形式表成

$$s_1 + ks_2 + \cdots + k^{p-1}s_p \quad (0 \leqslant s_i \leqslant k-1,\ \ i = 1, \cdots, p),$$

故由 (5) 卽得

$$\sum_{\nu=0}^{l-1} c_\nu\, \varphi_\nu(x_1, \cdots, x_p) \equiv 0\,,$$

此與假設相違. 由引理 2, l 個多項式 (4) 之 Wronskian

$$W(t) = \left| \frac{1}{\mu!} \left(\frac{d}{dt}\right)^\mu \varphi_\nu(t, t^k, \cdots, t^{k^{p-1}}) \right| \quad (\mu, \nu = 0, \cdots, l-1) \tag{6}$$

不恆爲 0. 但

$$\frac{d}{dt} = \frac{\partial}{\partial x_1} + kt^{k-1}\frac{\partial}{\partial x_2} + \cdots + k^{p-1}t^{k^{p-1}-1}\frac{\partial}{\partial x_p}$$

(右邊之運算係施行於 $x_1, \cdots, x_p$ 之多項式, 然後將所得結果中之 $x_1, \cdots, x_p$ 分別以 $t, t^k, \cdots, t^{k^{p-1}}$ 代入). 顯而易見

$$\left(\frac{d}{dt}\right)^\mu = f_1(t)\,\Delta^{(1)} + \cdots + f_r(t)\,\Delta^{(r)},$$

於此, r 僅依於 μ 及 p, $\Delta^{(1)}, \cdots, \Delta^{(r)}$ 爲階數不超過 μ 之微分運算, $f_1(t), \cdots,$

$f_r(t)$ 則為 t 之有理係數多項式. 將此代入 (6). 顯而易見，我們可將所得行列式寫成

$$W(t)=g_1(t)\,G^{(1)}(t,\cdots,t^{k^{p-1}})+\cdots+g_s(t)\,G^{(s)}(t,\cdots,t^{k^{p-1}})$$

之形式,於此, $G^{(1)},\cdots,G^{(s)}$ 為 $\varphi_0,\cdots,\varphi_{l-1}$ 的某些廣義 Wronskian, $g_1(t),\cdots,g_s(t)$ 為 t 之多項式. 因 $W(t)$ 不恆為 0, 故必有一 $G^{(i)}(t,\cdots,t^{k^{p-1}})$ 不恆為 0, 因而更有 $G^{(i)}(x_1,\cdots,x_p)$ 不恆為 0, 而吾人之引理即已證明.

引 4. 設 $p\geqslant 2$, $R(x_1,\cdots,x_p)$ 為具整係數之多項式, 且不恆為 0. 又設 R 關於 x_j 之次數為 $r_j(j=1,\cdots,p)$. 則存在一 l:

$$1\leqslant l\leqslant r_p+1 \tag{7}$$

及關於 $p-1$ 個變數 $x_1,\cdots,x_{p-1}$ 的微分運算 $\Delta_0,\cdots,\Delta_{l-1}$ (其各之階分別至多為 $0,\cdots,l-1$), 使得

(i) $$F(x_1,\cdots,x_p)=\left|\Delta_\mu\frac{1}{\nu!}\left(\frac{\partial}{\partial x_p}\right)^\nu R\right|,\quad(\mu,\nu=0,\cdots,l-1) \tag{8}$$

有整係數,且不恆為 0;

(ii) $F(x_1,\cdots,x_p)$ 可寫成

$$F(x_1,\cdots,x_p)=U(x_1,\cdots,x_{p-1})\,V(x_p), \tag{9}$$

於此, U 及 V 具有整係數, U 關於 x_j 之次數至多為 $lr_j(j=1,\cdots,p-1)$, V 之次數至多為 lr_p.

證: 將 R 表成

$$R(x_1,\cdots,x_p)=\varphi_0(x_p)\,\psi_0(x_1,\cdots,x_{p-1})+\cdots+\varphi_{l-1}(x_p)\,\psi_{l-1}(x_1,\cdots,x_{p-1})$$

之形式,於此, φ_ν 及 ψ_ν 為有理係數多項式, φ_ν 至多為 r_p 次, ψ_ν 關於 x_j 至多為 r_j 次 $(j=1,\cdots,p-1)$. 此項表法顯然是可能的,例如 $l-1=r_p$, $\varphi_\nu(x_p)==x_p^\nu$ 就能使之成立. 從所有這種表法中,我們選取一個表法, 其 l 為最小者. 則與此表示相應之

$$\varphi_0(x_p),\cdots,\varphi_{l-1}(x_p)$$

為線性獨立,否則若有

$$\varphi_{l-1}=d_0\varphi_0+\cdots+d_{l-2}\varphi_{l-2}$$

$(d_0,\cdots,d_{l-2}$ 為有理數),則

$$R=\varphi_0(\psi_0+d_0\,\psi_{l-1})+\cdots+\varphi_{l-2}(\psi_{l-2}+d_{l-2}\,\psi_{l-1}),$$

而 l 非爲最小者. 同理,

$$\psi_0(x_1,\cdots,x_{p-1}),\cdots,\psi_{l-1}(x_1,\cdots,x_{p-1})$$

爲線性獨立,且 $1\leqslant l\leqslant r_p+1$.

令 $W(x_p)$ 表 $\varphi_0(x_p),\cdots,\varphi_{l-1}(x_p)$ 之 Wronskian, 由引 2, W 爲一不恆爲 0 之有理係數多項式. 由引 3, 存在

$$\psi_0(x_1,\cdots,x_p),\cdots,\psi_{l-1}(x_1,\cdots,x_{p-1})$$

之一不恆爲 0 的廣義 Wronskian $G(x_1,\cdots,x_{p-1})$,

$$G(x_1,\cdots,x_{p-1})=|\,\Delta_\mu\,\psi_\nu(x_1,\cdots,x_{p-1})|\qquad(\mu,\nu=0,\cdots,l-1),$$

於此 $\Delta_0,\cdots,\Delta_{l-1}$ 爲形如 (3) 之微分運算(以 $p-1$ 代 p), 其各之階分別至多爲 $0,\cdots,l-1$. 將行列式 W, G 按行相乘,卽得

$$GW=\left|\sum_{\rho=0}^{l-1}\Delta_\mu\frac{1}{\nu!}\left(\frac{\partial}{\partial x_p}\right)^\nu\varphi_\rho(x_p)\,\psi_\rho(x_1,\cdots,x_{p-1})\right|=$$

$$=\left|\,\Delta_\mu\frac{1}{\nu!}\left(\frac{\partial}{\partial x_p}\right)^\nu R\,\right|\qquad(\mu,\nu=0,\cdots,l-1).$$

由是, $F(x_1,\cdots,x_p)=W(x_p)\;G(x_1,\cdots,x_{p-1})$ 已經寫成 (9) 的形式.

今往證明 (i):

因 R 之係數爲整數, 故 $F(x_1,\cdots,x_p)$ 之係數顯然爲整數; 又因 $U(x_1,\cdots,x_{p-1})$, $V(x_p)$ 皆不恆爲 0, 故 F 不恆爲 0, 此卽 (i).

再證明 (ii):

因

$$F(x_1,\cdots,x_p)=W(x_p)\,G(x_1,\cdots,x_{p-1})$$

左邊爲一整係數多項式, 而 W 及 G 皆爲有理係數多項式, 故必存在一有理數 g 使 $U(x_1,\cdots,x_{p-1})=gG(x_1,\cdots,x_{p-1})$ 及 $V(x_p)=g^{-1}\,W(x_p)$ 爲整係數多項式. (此乃顯而易見者,例如可取 g^{-1} 爲一分數,它使得 $g^{-1}\,W(x_p)$ 變爲一整係數多項式,且諸係數無異於 1 之公因子者). 再,因 W 爲一 l 階行列式,其元素爲一次數至多爲 r_p 之多項式,故 V 至多爲 lr_p 次. 同理, U 關於 x_j 至多爲 lr_j 次 $(j=1,\cdots,p-1)$. 此卽 (ii).

引 5. 設 R 滿足引 4 中之條件,又設 R 所有之係數之絕對值皆 $\leqslant B$. 則 (8) 中之 F 之所有係數之絕對值皆

$$\leqslant ((r_1+1)\cdots(r_p+1))^l\, l!\, B^l\, 2^{(r_1+\cdots+r_p)l}.$$

證: 因 R 爲一 $(r_1+1)\cdots(r_p+1)$ 項之多項式,其各形如

$$a_{s_1,\cdots,s_p}x_1^{s_1}\cdots x_p^{s_p},$$

於此, $|a_{s_1,\cdots,s_p}|\leqslant B$. (8) 式右邊之行列式可以寫成 $((r_1+1)\cdots(r_p+1))^l$ 個行列式之和,各行列式之元素形如

$$a_{s_1,\cdots,s_p}\Delta_\mu\frac{1}{\nu!}\left(\frac{\partial}{\partial x_p}\right)^\nu x_1^{s_1}\cdots x_p^{s_p},$$

於此, $s_1,\cdots,s_p$ 依照原行列式按行或按列展開而依於 μ 或 ν.

但

$$\Delta_\mu\frac{1}{\nu!}\left(\frac{\partial}{\partial x_p}\right)^\nu x_1^{s_1}\cdots x_p^{s_p}=Ax_1^{t_1}\cdots x_p^{t_p},\quad t_1\leqslant s_1,\cdots,t_p\leqslant s_p,$$

而係數 A 或爲 0, 或等於

$$\binom{s_1}{t_1}\cdots\binom{s_p}{t_p}\leqslant 2^{s_1+\cdots+s_p}\leqslant 2^{r_1+\cdots+r_p}.$$

故各行列式的展式中每一項之絕對值皆

$$\leqslant (B\,2^{r_1+\cdots+r_p})^l.$$

因一行列式共有 $l!$ 項,行列式之數目爲 $((r_1+1)\cdots(r_p+1))^l$, 故引理卽已證明.

2. 設 $P(x_1,\cdots,x_p)$ 爲一不恆爲 0 之多項式. 設 $\alpha_1,\cdots,\alpha_p$ 爲任意實數, 又設 $r_1,\cdots,r_p$ 爲任意正數.

定義 3. 設

$$P(\alpha_1+y_1,\cdots,\alpha_p+y_p)=\sum_{j_1=0}^{\infty}\cdots\sum_{j_p=0}^{\infty}c(j_1,\cdots,j_p)\,y_1^{j_1}\cdots y_p^{j_p},$$

則

$$\theta=\min_{\substack{j_1,\cdots,j_p\geqslant 0\\ c(j_1,\cdots,j_p)\neq 0}}\left(\frac{j_1}{r_1}+\cdots+\frac{j_p}{r_p}\right)$$

稱爲 P 在點 $(\alpha_1,\cdots,\alpha_p)$ 關於 $r_1,\cdots,r_p$ 之指標,記作 index P.

換言之，多項式 P 在一點 $(\alpha_1,\cdots,\alpha_p)$ 關於 $r_1,\cdots,r_p$ 之指標，乃是指 $\frac{j_1}{r_1}+\cdots+\frac{j_p}{r_p}$ 對於所有使得

$$\left(\frac{\partial}{\partial x_1}\right)^{j_1}\cdots\left(\frac{\partial}{\partial x_p}\right)^{j_p}P(\alpha_1,\cdots,\alpha_p)\neq 0$$

之諸非負整數 $j_1,\cdots,j_p$ 所取之最小數值.

顯然有 $\theta\geqslant 0$, 而 $\theta=0$ 即謂 $P(\alpha_1,\cdots,\alpha_p)\neq 0$ 反之亦然.

引 6. 設 $k_1\geqslant 0,\cdots,k_p\geqslant 0$, 又設

$$\left(\frac{\partial}{\partial x_1}\right)^{k_1}\cdots\left(\frac{\partial}{\partial x_p}\right)^{k_p}P(x_1,\cdots,x_p)$$

不恆為 0, 則其在 $(\alpha_1,\cdots,\alpha_p)$ 關於 $r_1,\cdots,r_p$ 之指標必

$$\geqslant\theta-\frac{k_1}{r_1}-\cdots-\frac{k_p}{r_p}.$$

此可由 θ 之定義立刻得出. 下之引理亦係顯而易見者:

引 7. 設 $P(x_1,\cdots,x_p)$, $Q(x_1,\cdots,x_p)$ 為多項式,皆不恆為 0. 又設所有之指標皆是在同一點 $(\alpha_1,\cdots,\alpha_p)$ 關於同一組數 $r_1,\cdots,r_p$ 而做成者. 則有

$$\operatorname{index}(P+Q)\geqslant\min(\operatorname{index}P,\operatorname{index}Q),\tag{10}$$

$$\operatorname{index}PQ=\operatorname{index}P+\operatorname{index}Q.\tag{11}$$

且若 P 為 $x_1,\cdots,x_{p-1}$ 之一多項式, Q 為 x_p 之一多項式, 而 P 之指標係在 $(\alpha_1,\cdots,\alpha_{p-1})$ 關於 $r_1,\cdots,r_{p-1}$ 作成, Q 之指標係在 α_p 關於 r_p 作成, 則 (11) 式仍成立.

設 $r_1,\cdots,r_m$ 與 $B\geqslant 1$ 為一組給定之正整數. $R(x_1,\cdots,x_m)$ 為滿足下列條件之多項式:

(a) R 具有整係數,且不恆為 0;

(b) R 關於 x_j 至多為 r_j 次, $j=1,\cdots,m$;

(c) R 之係數之絕對值 $\leqslant B$.

所有如是之 R 成為一集,記作

$$\mathfrak{R}_m=\mathfrak{R}_m(B;r_1,\cdots,r_m).$$

設 $q_1,\cdots,q_m$ 為一組正整數, $h_1,\cdots,h_m$ 為一組整數, $(h_j,q_j)=1$, $j=1,\cdots,m$.

令 $\theta(R)$ 表示 R 在 $\left(\frac{h_1}{q_1},\cdots,\frac{h_m}{q_m}\right)$ 關於 $r_1,\cdots,r_m$ 之指標。記

$$\Theta_m(B;\ q_1,\cdots,q_m;\ r_1,\cdots,r_m)=\underset{\substack{R\in\mathfrak{R}_m\\(h_j,\,q_j)=1}}{u.\,b.}\,\theta(R)\,, \tag{12}$$

卽 $\theta(R)$ 對於 $\mathfrak{R}_m$ 中所有之 R 及分別與 $q_1,\cdots,q_m$ 互素之所有整數 $h_1,\cdots,h_m$ 所取之上界。

在下面，我們的主要目的卽在某種條件下估計此 $\Theta_m(B;q_1,\cdots,q_m;r_1,\cdots,r_m)$ 之値。我們要注意 (12) 中 $r_1,\cdots,r_m$ 之雙重意義。

在估計 $\Theta_m(B;q_1,\cdots,q_m;r_1,\cdots,r_m)$ 時，我們用的是歸納法。下述的引理卽爲歸納法準備一遞推過程。

引 8. 設 $0<\delta<1$, $p\geqslant 2$, $r_1,\cdots,r_p$ 爲滿足關係

$$r_p>10\,\delta^{-1},\quad r_{j-1}/r_j>\delta^{-1},\quad j=2,\cdots,p \tag{13}$$

之一組正整數，$q_1,\cdots,q_p$ 爲任意一組正整數，則

$$\Theta_p(B;\ q_1,\cdots,q_p;\ r_1,\cdots,r_p)\leqslant 2\max_{1\leqslant l\leqslant r_p+1}(\Phi+\Phi^{1/2}+\delta^{1/2})\,, \tag{14}$$

於此

$$\Phi=\Theta_1(M;\ q_p;\ lr_p)+\Theta_{p-1}(M;\ q_1,\cdots,q_{p-1};\ lr_1,\cdots,lr_{p-1})\,, \tag{15}$$

$$M=(r_1+1)^{pl}\,l!\,B^l\,2^{plr_1}.$$

證：對 $\mathfrak{R}_p(B;r_1,\cdots,r_p)$ 中之任一多項式 $R(x_1,\cdots,x_p)$，由引 4，知存在一 l: $1\leqslant l\leqslant r_p+1$ 及一多項式 $F(x_1,\cdots,x_p)$ 具有引 4 中之性質 (i) 及 (ii)。由引 5，F 之係數的絕對値

$$\leqslant((r_1+1)\cdots(r_p+1))^l\,l!\,B^l\,2^{(r_1+\cdots+r_p)l}<M.$$

因

$$F=U(x_1,\cdots,x_{p-1})\,V(x_p)$$

中之 U,V 皆具有整係數，故 U 及 V 之係數皆 $<M$。

$U(x_1,\cdots,x_{p-1})$ 關於 x_j 之次數至多爲 lr_j $(j=1,\cdots,p-1)$。由定義，$U(x_1,\cdots,x_{p-1})$ 屬於集

$$\mathfrak{R}_{p-1}(M;\ lr_1,\cdots,lr_{p-1})\,.$$

因之，$U(x_1,\cdots,x_{p-1})$ 在 $\left(\frac{h_1}{q_1},\cdots,\frac{h_{p-1}}{q_{p-1}}\right)$ 關於 $lr_1,\cdots,lr_p$ 的指標

$$\leqslant \Theta_{p-1}(M; q_1, \cdots, q_{p-1}; lr_1, \cdots, lr_{p-1}).$$

由定義 3, U 在此點關於 $r_1, \cdots, r_{p-1}$ 之指標

$$\leqslant l\,\Theta_{p-1}(M; q_1, \cdots, q_{p-1}; lr_1, \cdots, lr_{p-1});$$

同理, $V(x_p)$ 屬於集 $\Re_1(M; lr_p)$, 其在 $\frac{h_p}{q_p}$ 關於 r_p 之指標

$$\leqslant l\,\Theta_1(M; q_p; lr_p).$$

由引 7, $F = UV$ 在 $\left(\frac{h_1}{q_1}, \cdots, \frac{h_p}{q_p}\right)$ 關於 $r_1, \cdots, r_p$ 之指標等於 U 及 V 之指標和,故

$$\text{index } F \leqslant l\Phi, \tag{16}$$

Φ 之定義見 (15).

下面我們將根據 (8), 設法求出 F 之指標的一下界,而且是以 R 之指標 θ 表出者. 由是,將所得結果與 (16) 相較,卽得出我們的引理.

設關於 $x_1, \cdots, x_{p-1}$ 之微分運算

$$\Delta = \frac{1}{i_1! \cdots i_{p-1}!}\left(\frac{\partial}{\partial x_1}\right)^{i_1} \cdots \left(\frac{\partial}{\partial x_{p-1}}\right)^{i_{p-1}}$$

之階 $\omega = i_1 + \cdots + i_{p-1} \leqslant l - 1$. 若多項式

$$\Delta \frac{1}{\nu!}\left(\frac{\partial}{\partial x_p}\right)^{\nu} R(x_1, \cdots, x_p)$$

不恆爲 0, 則由引 6, 其在 $\left(\frac{h_1}{q_1}, \cdots, \frac{h_p}{q_p}\right)$ 關於 $r_1, \cdots, r_p$ 之指標

$$\geqslant \theta - \frac{i_1}{r_1} - \cdots - \frac{i_{p-1}}{r_{p-1}} - \frac{\nu}{r_p} \geqslant \theta - \frac{\omega}{r_{p-1}} - \frac{\nu}{r_p}.$$

但因 $l \leqslant r_p + 1$, 故由 (13), 卽得 $\omega/r_{p-1} \leqslant (l-1)/r_{p-1} \leqslant r_p/r_{p-1} < \delta$. 由是可知此指標

$$\geqslant \max(0, \theta - \nu/r_p) - \delta.$$

將 (8) 式右邊之行列式展開,我們卽將 F 表示成爲一和,其項數 $\leqslant l!$, 其一般項形如

$$\pm (\Delta_{\mu_0} R)\left(\Delta_{\mu_1} \frac{1}{1!} \frac{\partial}{\partial x_p} R\right) \cdots \left(\Delta_{\mu_{l-1}} \frac{1}{(l-1)!}\left(\frac{\partial}{\partial x_p}\right)^{l-1} R\right),$$

於此，$\Delta_{\mu_0},\cdots,\Delta_{\mu_{l-1}}$ 爲關於 $x_1,\cdots,x_{p-1}$ 之微分運算,其階至多爲 $l-1$. 由引7(11)，如是之項(若不恆爲 0)之指標必

$$\geqslant \sum_{\nu=0}^{l-1} \max(0, \theta-\nu/r_p) - l\delta .$$

由 (10)，

$$\text{index}\, F \geqslant \sum_{\nu=0}^{l-1} \max(0, \theta-\nu/r_p) - l\,\delta .$$

若 $\theta r_p < 10$，則引理顯然成立.

若 $10 \leqslant \theta r_p < l$，則

$$\sum_{\nu=0}^{l-1} \max(0, \theta-\nu/r_p) = r_p^{-1} \sum_{0\leqslant\nu\leqslant\theta r_p} (\theta r_p - \nu) \geqslant$$

$$\geqslant \frac{1}{2} r_p^{-1} [\theta\, r_p]^2 \geqslant \frac{1}{3} r_p\, \theta^2 .$$

若 $\theta r_p \geqslant l$，則

$$\sum_{\nu=0}^{l-1} \max(0, \theta-\nu/r_p) = \sum_{\nu=0}^{l-1} (\theta-\nu/r_p) \geqslant \frac{1}{2}\, l\theta .$$

總之,得

$$\text{index}\, F \geqslant \min\left(\frac{1}{2}\, l\,\theta, \frac{1}{3}\, r_p\, \theta^2\right) - l\,\delta .$$

將此與 (16) 相較,卽得

$$\min\left(\frac{1}{2}\, l\theta, \frac{1}{3}\, r_p\, \theta^2\right) \leqslant l(\varPhi + \delta) .$$

若 $\theta \leqslant 2(\varPhi+\delta)$，則引理已明. 若 $\theta \geqslant 2(\varPhi+\delta)$，則

$$\frac{1}{3}\, r_p\, \theta^2 \leqslant l(\varPhi+\delta) \leqslant (r_p+1)\,(\varPhi+\delta) .$$

由 (13)，$r_p + 1 < \frac{4}{3} r_p$，故由上式卽得

$$\theta < 2(\varPhi+\delta)^{1/2} \leqslant 2(\varPhi^{1/2} + \delta^{1/2}) .$$

吾人之引理卽已證明.

引 9. 設 m 爲正整數,

$$0 < \delta < m^{-1}, \tag{17}$$

又設 $r_1,\cdots,r_m$ 及 $q_1,\cdots,q_m$ 爲兩組正整數,滿足關係

$$r_m > 10\,\delta^{-1},\quad r_{j-1}/r_j > \delta^{-1},\quad j=2,\cdots,m, \tag{18}$$

$$\log q_1 > \delta^{-1}\,m(2m+1), \tag{19}$$

$$r_j \log q_j \geqslant r_1 \log q_1,\quad j=2,\cdots,m. \tag{20}$$

則

$$\Theta_m(q_1^{\delta r_1};\ q_1,\cdots,q_m;\ r_1,\cdots,r_m) < 10^m\,\delta^{(1/2)^m}. \tag{21}$$

證: 我們在 m 上施行歸納法來證明本引理.

當 $m=1$, 由 θ 之定義, 多項式 $R(x_1)$ 可爲 $(x_1-h_1/q_1)^{\theta r_1}$ 除盡. 因 $(h_1,q_1)=1$, 故由定理 1.13.2,

$$R(x_1)=(q_1x_1-h_1)^{\theta r_1}\,Q(x_1),$$

於此 $Q(x_1)$ 爲一整係數多項式. 故 $R(x_1)$ 之最高項之係數必爲 $q_1^{\theta r_1}$ 之一整數倍. 由是卽得

$$q_1^{\theta r_1} \leqslant q_1^{\delta r_1}.$$

卽 $\theta\leqslant\delta\leqslant 10\,\delta^{1/2}$. 故引理對 $m=1$ 成立.

今設引理對 $m=p-1$ $(p\geqslant 2)$ 成立. 而證明其對 $m=p$ 也成立. 我們現在估計引 8 中之 M 及 Φ(注意引 9 之條件強於引 8 之條件).

因 $l\leqslant r_p+1<r_1+1\leqslant 2^{r_1}$, 故得

$$M=(r_1+1)^{pl}\,l!\,2^{plr_1}\,q_1^{\delta l r_1}\leqslant((r_1+1)^p\,l\,2^{pr_1}\,q_1^{\delta r_1})^l<$$

$$<(2^{(2p+1)r_1}\,q_1^{\delta r_1})^l<(e^{(2p+1)r_1}\,q_1^{\delta r_1})^l.$$

由 (19) (令 $m=p$), 我們有 $2p+1<\delta p^{-1}\log q_1$, 代入上式,卽得

$$M<q_1^{\delta_1 l r_1},$$

於此,

$$\delta_1=\delta(1+p^{-1}). \tag{22}$$

由是卽得

$$\Theta_1(M;\ q_p;\ lr_p)\leqslant\Theta_1(q_1^{\delta_1 l r_1};\ q_p;\ lr_p), \tag{23}$$

$$\Theta_{p-1}(M;\ q_1,\cdots,q_{p-1};\ lr_1,\cdots,lr_{p-1})\leqslant$$

$$\leqslant \Theta_{p-1}(q_1^{\delta_1 lr_1}; q_1, \cdots, q_{p-1}; lr_1, \cdots, lr_{p-1}). \tag{24}$$

因引理對於 $m=1$ 已證明成立,故 (23) 之右邊

$$< 10\,\delta_1^{1/2}. \tag{25}$$

今運用歸納法之假定來估計 (24) 之右邊. 將 (24) 之右邊與 (21) 之左邊相較,所不同者爲 δ 之位置換爲 δ_1, r_i 之位置換於 lr_i. 因 $\delta_1 > \delta$, 故在引理之假設中,除 (17) 外,餘皆滿足. 然欲證明與 (17) 相類之不等式, 亦卽證明

$$\delta_1 < (p-1)^{-1},$$

只須注意由 (17) (命 $m=p$) $\delta < p^{-1}$ 及由 (22) $\delta_1 = \delta(1+p^{-1})$ 立可得出. 故得

$$\Theta_{p-1}(q_1^{\delta_1 lr_1}; q_1, \cdots, q_{p-1}; lr_1, \cdots, lr_{p-1}) < 10^{p-1}\,\delta_1^{(1/2)^{p-1}}. \tag{26}$$

由 (15), (25) 及 (26), 卽得(因 $\delta_1 < 2\delta$ 及 $p \geqslant 2$)

$$\Phi < 10\,\delta_1^{1/2} + 10^{p-1}\,\delta_1^{(1/2)^{p-1}} <$$
$$< 3(10^{p-1}\,\delta^{(1/2)^{p-1}}).$$

由 (14), 卽得

$$\Theta_p(q_1^{\delta r_1}; q_1, \cdots, q_p; r_1, \cdots, r_p) < 2(3(10^{p-1}\,\delta^{(1/2)^{p-1}}) + 3^{1/2}10^{(p-1)/2}\delta^{(1/2)^p} + \delta^{1/2}) <$$
$$< 2\left(\frac{3}{10} + \frac{3^{1/2}}{10^{3/2}} + \frac{1}{10^{1/2}}\right)10^p\,\delta^{(1/2)^p} <$$
$$< 10^p\,\delta^{(1/2)^p}.$$

故引理對於 $m=p$ 亦成立. 吾人之引理卽已證明.

3. 下面,我們將證明一簡單之引理.

引 10. 設 $r_1, \cdots, r_m$ 爲任意正整數, $\lambda > 0$. 則不定方程

$$\frac{j_1}{r_1} + \cdots + \frac{j_m}{r_m} \leqslant \frac{1}{2}(m-\lambda), \quad 0 \leqslant j_1 \leqslant r_1, \cdots, \quad 0 \leqslant j_m \leqslant r_m \tag{27}$$

之解答之組數

$$\leqslant 2m^{1/2}\lambda^{-1}(r_1+1)\cdots(r_m+1).$$

證: 我們現用歸納法來證明本引理.

引理當 $m=1$ 時顯然成立. 今假定引理對 $m-1$ 成立. 顯而易見, 我們可以假定 $\lambda > 2m^{1/2}$. 對於一固定之 j_m, 取 $\lambda' = \lambda - 1 + 2\, j_m/r_m$, 則因 $\lambda > 2m^{1/2} > 1$, $0 \leqslant j_m \leqslant r_m$, 故 $\lambda' > 0$, 由是 (27) 可寫成

$$\frac{j_1}{r_1} + \cdots + \frac{j_{m-1}}{r_{m-1}} \leqslant \frac{1}{2}(m-1-\lambda'), \quad 0 \leqslant j_i \leqslant r_i, \quad i = 1, \cdots, m-1.$$

由歸納法假定, (27) 之解數

$$\leqslant \sum_{j_m=0}^{r_m} 2(m-1)^{1/2}(\lambda - 1 + 2j_m/r_m)^{-1}(r_1+1)\cdots(r_{m-1}+1).$$

故欲證明引理, 只須證明對任何正整數 r 與 m 以及任何 $\lambda > 2m^{1/2}$, 有

$$\sum_{j=0}^{r}(\lambda - 1 + 2j/r)^{-1} < \lambda^{-1}(m-1)^{-1/2}\, m^{1/2}(r+1)$$

即可.

若 r 為偶數, 令 $j = \frac{1}{2}r + k$, 則上式變成

$$\sum_{k=-\frac{r}{2}}^{r/2}(\lambda + 2k/r)^{-1} = \lambda^{-1} + \sum_{k=1}^{r/2} 2\lambda(\lambda^2 - 4k^2/r^2)^{-1} \leqslant$$

$$\leqslant \lambda^{-1} + \sum_{k=1}^{r/2} 2\lambda(\lambda^2 - 1)^{-1} \leqslant$$

$$\leqslant (r+1)\lambda^{-1}(1-\lambda^{-2})^{-1}.$$

因 $1 - \lambda^{-2} > 1 - \frac{1}{4}m^{-1} > (1-m^{-1})^{1/2}$, 故我們的引理即已證明.

若 r 為奇數上之結果同樣得到證明.

4. 在結束定理 1 的證明之前, 我們尚須證明下引(引 11). 實際上, 在定理 1 之最後證明中, 僅有此引發生作用, 前面所述諸引皆係為引 11 之證明而準備者. 在陳述引 11 之前, 我們先注意, 若定理 1 對於代數整數成立, 則其對一般代數數亦成立. 事實上, 設 α 為一代數數, 但非代數整數, 對此 α 有一 $\kappa > 2$ 使

$$\left| \alpha - \frac{x}{y} \right| < \frac{1}{y^{\kappa}}, \quad (y > 0)$$

有無限多對整數解 (x, y). 易知存在一自然數 q, 使 $q\alpha$ 為一代數整數. 由是

$$\left| q\alpha - \frac{qx}{y} \right| = \left| q\alpha - \frac{x'}{y} \right| < \frac{q}{y^{\kappa}}$$

有無限多對解. 但當 y 甚大時,上式即表明

$$\left| q\alpha - \frac{x'}{y} \right| < \frac{1}{y^{2+\frac{1}{2}(\kappa-2)}}$$

有無限多對整數解 (x', y). 而由定理 1, 此爲不可能者.

在下面之敍述中,常設 α 爲一代數整數,其所滿足之方程爲

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n, \tag{28}$$

式中 a_i 爲不同時爲 0 之整數. 令

$$A = \max(|a_i|, i = 1, \cdots, n). \tag{29}$$

我們又選取 $m, \delta, q_1, h_1, \cdots, q_m, h_m, r_1, \cdots, r_m$ 滿足下列條件:

$$0 < \delta < m^{-1}; \tag{30}$$

$$10^m \delta^{(1/2)^m} + 2(1 + 3\delta) n m^{1/2} < \frac{1}{2} m; \tag{31}$$

$$r_m > 10\delta^{-1}, \quad r_{j-1}/r_j > \delta^{-1}, \quad j = 2, \cdots, m; \tag{32}$$

$$\delta^2 \log q_1 > 2m + 1 + 2m \log(1 + A) + 2m \log(1 + |\alpha|); \tag{33}$$

$$r_j \log q_j \geqslant r_1 \log q_1. \tag{34}$$

注意: 引 9 中之條件在此皆成立.

定義 $\lambda, \gamma, \eta, B_1$ 如

$$\lambda = 4(1 + 3\delta) n m^{1/2}; \tag{35}$$

$$\gamma = \frac{1}{2}(m - \lambda); \tag{36}$$

$$\eta = 10^m \delta^{(1/2)^m}; \tag{37}$$

$$B_1 = \left[q_1^{\delta r_1} \right]. \tag{38}$$

由 (31), (35), (36) 及 (37) 可知

$$\eta < \gamma. \tag{39}$$

注意: $r_1 > 10$, 由 (33), $q_1^{\delta^2} > e^{2m+1}$, 故 B_1 甚大,特別,有 $q_1^{\frac{1}{2}\delta r_1} < B_1$.

引 11. 設 (30) – (34) 皆成立, 又設整數 $h_1, \cdots, h_m$ 分別與 $q_1, \cdots, q_m$ 互

素. 則存在整係數多項式 $Q(x_1,\cdots,x_m)$, 其關於 x_j 之次數至多爲 $r_j(j=1,\cdots,m)$, 使得

(i) Q 在 $(\alpha,\cdots,\alpha)$ 關於 $r_1,\cdots,r_m$ 之指標至少爲 $\gamma-\eta$;

(ii) $Q(h_1/q_1,\cdots,h_m/q_m)\neq 0$;

(iii) 設 $i_1,\cdots,i_m$ 爲任意非負整數,則對

$$Q_{i_1,\cdots,i_m}(x_1,\cdots,x_m)=\frac{1}{i_1!\cdots i_m!}\left(\frac{\partial}{\partial x_1}\right)^{i_1}\cdots\left(\frac{\partial}{\partial x_m}\right)^{i_m}Q,$$

我們有

$$|Q_{i_1,\cdots,i_m}(\alpha,\cdots,\alpha)|<B_1^{1+3\delta}. \tag{40}$$

證: 我們現考慮所有形如

$$W(x_1,\cdots,x_m)=\sum_{s_1=0}^{r_1}\cdots\sum_{s_m=0}^{r_m}c(s_1,\cdots,s_m)\,x_1^{s_1}\cdots x_m^{s_m} \tag{41}$$

之多項式 $W(x_1,\cdots,x_m)$, 於此, 係數 $c(s_1,\cdots,s_m)$ 分別互相無關地取過所有滿足條件

$$0\leqslant c(s_1,\cdots,s_m)\leqslant B_1 \tag{42}$$

之整數. 如是之多項式之數目顯然等於

$$N=(B_1+1)^r, \tag{43}$$

於此,

$$r=(r_1+1)\cdots(r_m+1). \tag{44}$$

對於每一如是之 W, 我們來考慮所有之導數

$$W_{j_1,\cdots,j_m}(x_1,\cdots,x_m)=\frac{1}{j_1!\cdots j_m!}\left(\frac{\partial}{\partial x_1}\right)^{j_1}\cdots\left(\frac{\partial}{\partial x_m}\right)^{j_m}W,$$

其 $j_1,\cdots,j_m$ 滿足條件

$$0\leqslant j_1\leqslant r_1,\cdots,0\leqslant j_m\leqslant r_m,\ \frac{j_1}{r_1}+\cdots+\frac{j_m}{r_m}\leqslant\gamma \tag{45}$$

者. 由引 10 及 (36), 如是之導數之數目 D 滿足關係

$$D\leqslant 2m^{1/2}\lambda^{-1}r. \tag{46}$$

對每一如是之導數,我們作單變數多項式

$$W_{j_1,\cdots,j_m}(x,\cdots,x),$$

並以 $f(x)$ 除之,而將所得餘式記作

$$T_{i_1,\cdots,i_m}(W;x).$$

上式顯然為一整係數多項式,其次數至多為 $n-1$.

我們現來估計任何這種餘式的係數之大小. 顯而易見,多項式 $W_{i_1,\cdots,i_m}(x_1,\cdots,x_m)$ 之每一係數的絕對值

$$\leqslant 2^{r_1+\cdots+r_m}B_1\leqslant 2^{mr_1}B_1<B_1^{1+\delta},$$

蓋由 (33), $mr_1\log 2<\frac{1}{2}\delta^2 r_1\log q_1$. 當 $x_1,\cdots,x_m$ 全部代以 x, 此多項式中某些項可能合併. 因此多項式至多有 r 項,故由上式, $W_{i_1,\cdots,i_m}(x,\cdots,x)$ 之係數的絕對值 $<rB_1^{1+\delta}$. 但

$$r=(r_1+1)\cdots(r_m+1)\leqslant 2^{r_1+\cdots+r_m}\leqslant 2^{mr_1}<B_1^{\delta},$$

故 $rB_1^{1+\delta}<B_1^{1+2\delta}$.

設

$$W_{i_1,\cdots,i_m}(x,\cdots,x)=\omega_s x^s+\omega_{s-1}x^{s-1}+\cdots+\omega_0.$$

今用 $f(x)$ 除上式. 在第一次除時(假定 $s\geqslant n$), 乃係從上式減去 $\omega_s x^{s-n}f(x)$, 結果得出一新多項式,其係數或形如 $\omega_\nu-a_{s-\nu}\omega_s$, 或形如 ω_ν. 故此新多項式之係數的絕對值 $\leqslant(1+A)B_1^{1+2\delta}$. 此項手續可再繼續進行, 每進行一次, 所得新多項式之係數的絕對值之上界卽引進一 $(1+A)$ 之因子. 然此項手續至多經過 $s-n+1$ 次必告終止,故餘式 $T_{i_1,\cdots,i_m}(W;x)$ 之係數的絕對值

$$\leqslant(1+A)^{s-n+1}B_1^{1+2\delta}.$$

由 $s\leqslant r_1+\cdots+r_m\leqslant mr_1$ 及 (33), 卽得上式

$$\leqslant(1+A)^{mr_1}B_1^{1+2\delta}<B_1^{1+3\delta}. \tag{47}$$

因對於一個 W, 我們可以得到一組 $T_{i_1,\cdots,i_m}(W;x)$, 其中所含多項式的數目為 D. 同時,每一多項式至多有 n 個係數, 故由 (47), 如是之組至多有

$$(1+2B_1^{1+3\delta})^{nD}$$

個各不相同. 但由 (46) 及 (35),

$$(1+3\delta)nD\leqslant 2(1+3\delta)nm^{1/2}\lambda^{-1}r=\frac{1}{2}r,$$

故不同之組的數目

$$\leqslant (1+2B_1^{1+3\delta})^{nD} < (2+2B_1)^{r/2} < (1+B_1)^r.$$

由 (43), 我們可以看出,必然存在兩個形如 (41) 之不同之多項式 W' 及 W'', 使得

$$W'_{i_1,\cdots,i_m}(x,\cdots,x) - W''_{i_1,\cdots,i_m}(x,\cdots,x)$$

對於所有滿足 (45) 之 $j_1,\cdots,j_m$ 皆能為 $f(x)$ 除盡. 令 $W^* = W' - W''$, 則此卽謂所有與 (45) 相應之導數

$$W^*_{i_1,\cdots,i_m}(x,\cdots,x)$$

當 $x_1 = \cdots = x_m = \alpha$ 時為 0. 因而 W^* 在 $(\alpha,\cdots,\alpha)$ 關於 $r_1,\cdots,r_m$ 之指標至少為 γ. W^* 之係數皆為整數,且不同時為 0, 其絕對值不超過 B_1.

我們現在來運用引 9. W^* 顯然滿足 $\mathfrak{R}_m(B_1; r_1,\cdots,r_m)$之定義中的條件(a), (b), (c), 故屬於 $\mathfrak{R}_m(q_1^{\delta r_1}; r_1,\cdots,r_m)$. 由 (37) 及引 9, W^* 在 $(h_1/q_1,\cdots,h_m/q_m)$ 關於 $r_1,\cdots,r_m$ 之指標 $<\eta$. 故必存在一組 $k_1,\cdots,k_m$ 滿足條件

$$\frac{k_1}{r_1} + \cdots + \frac{k_m}{r_m} < \eta,$$

使得

$$Q(x_1,\cdots,x_m) = \frac{1}{k_1!\cdots k_m!}\left(\frac{\partial}{\partial x_1}\right)^{k_1}\cdots\left(\frac{\partial}{\partial x_m}\right)^{k_m} W^*$$

在點 $(h_1/q_1,\cdots,h_m/q_m)$ 不為 0, 此卽 (ii). (i) 可由引 6 及上式立刻得出.

因 W^* 之係數的絕對值 $\leqslant B_1$, 故 Q 之係數的絕對值

$$\leqslant 2^{r_1+\cdots+r_m} B_1 \leqslant 2^{mr_1} B_1 < B_1^{1+\delta}.$$

因而

$$Q_{i_1,\cdots,i_m}(x_1,\cdots,x_m)$$

之係數的絕對值 $\leqslant 2^{mr_1} B_1^{1+\delta} < B_1^{1+2\delta}$. 注意 (33), 由此卽得

$$|Q_{i_1,\cdots,i_m}(\alpha,\cdots,\alpha)| < B_1^{1+2\delta}(1+|\alpha|)^{r_1+\cdots+r_m} <$$

$$< B_1^{1+3\delta},$$

此卽 (iii). 由是,吾人之引理卽已證明.

5. 定理 1 之證明: 我們假定有一 $\kappa > 2$ 使得不等式

$$\left| \alpha - \frac{h}{q} \right| < \frac{1}{q^{\kappa}} \qquad (q > 0) \tag{48}$$

有無限多組整數解 (h, q). 因 α 非有理數,故可假定其中有無限多組解滿足關係 $(h, q) = 1$. 蓋若不然,則當 q 無限增大時, α 將與某一固定之有理數無限接近,即等於該有理數.

我們先選 m, 使 $m^{1/2} > 4n$, 及

$$\frac{2m}{m - 4nm^{1/2}} < \kappa, \tag{49}$$

因 $\kappa > 2$, 故此為可能. 再取 $\delta > 0$ 甚小,使

$$m - 4(1 + 3\delta)\, nm^{1/2} - 2\eta > 0,$$

因由 (37), η 隨 δ 趨於 0, 故此為可能. 此即 (31). 更取 δ 甚小, 使之旣滿足上式,又滿足 (30), 且滿足

$$\frac{2m(1+4\delta)}{m - 4(1+3\delta)nm^{1/2} - 2\eta} < \kappa, \tag{50}$$

由 (49), 此乃可能者. 由 γ 與 η 之定義 ((36) 及 (37)), 上式可寫成

$$\frac{m(1+4\delta)}{\gamma - \eta} < \kappa. \tag{51}$$

在旣經選定 m 與 δ 之後, 我們先來選取 (48) 之一組解 (h_1, q_1), 使得 $(h_1, q_1) = 1$, 且 q_1 甚大,滿足條件 (33). 然後再選取另外的解 $(h_2, q_2), \cdots, (h_m, q_m)$, $(h_j, q_j) = 1$ $(j = 2, \cdots, m)$, 使得

$$\frac{\log q_j}{\log q_{j-1}} > \frac{2}{\delta} \qquad (j = 2, \cdots, m). \tag{52}$$

再選取整數 r_1, 使

$$r_1 > \frac{10 \log q_m}{\delta \log q_1}, \tag{53}$$

然後定義 $r_2, \cdots, r_m$:

$$\frac{r_1 \log q_1}{\log q_j} \leqslant r_j < 1 + \frac{r_1 \log q_1}{\log q_j} \qquad (j = 2, \cdots, m). \tag{54}$$

故 (34) 成立. 由上式及 (53),

$$r_m \geqslant \frac{r_1 \log q_1}{\log q_m} > 10\,\delta^{-1},$$

又由 (54) 及 (53),

$$\frac{r_j \log q_j}{r_1 \log q_1} < 1 + \frac{\log q_j}{r_1 \log q_1} \leqslant 1 + \frac{\log q_m}{r_1 \log q_1} < 1 + \frac{1}{10}\,\delta. \tag{55}$$

故由 (54) 及 (52), 卽得

$$\frac{r_{j-1}}{r_j} > \frac{\log q_j}{\log q_{j-1}}\left(1+\frac{1}{10}\,\delta\right)^{-1} > \delta^{-1}.$$

由是 (32) 成立.

由引 11, 存在一多項式 $Q(x_1,\cdots,x_m)$ 具有該引理中之性質 (i), (ii) 及 (iii). 因 Q 之係數爲整數,其關於 x_j 至多爲 r_j 次 $(j=1,\cdots,m)$, 故由 (55), 卽得

$$\left| Q\left(\frac{h_1}{q_1},\cdots,\frac{h_m}{q_m}\right)\right| \geqslant q_1^{-r_1}\cdots q_m^{-r_m} > q_1^{-mr_1(1+\delta)}. \tag{56}$$

另一方面,我們有

$$Q\left(\frac{h_1}{q_1},\cdots,\frac{h_m}{q_m}\right) =$$

$$= \sum_{i_1=0}^{r_1}\cdots\sum_{i_m=0}^{r_m} Q_{i_1,\cdots,i_m}(\alpha,\cdots,\alpha)\left(\frac{h_1}{q_1}-\alpha\right)^{i_1}\cdots\left(\frac{h_m}{q_m}-\alpha\right)^{i_m},$$

由引 11, 上式右邊其滿足

$$\frac{i_1}{r_1}+\cdots+\frac{i_m}{r_m} < \gamma-\eta$$

之項皆爲 0. 對所有其餘之項,由 (54), 我們有

$$\left|\left(\frac{h_1}{q_1}-\alpha\right)^{i_1}\cdots\left(\frac{h_m}{q_m}-\alpha\right)^{i_m}\right| < \frac{1}{(q_1^{i_1}\cdots q_m^{i_m})^{\kappa}} \leqslant q_1^{-r_1(\gamma-\eta)\kappa}.$$

由引 11 之 (iii),

$$\left| Q\left(\frac{h_1}{q_1},\cdots,\frac{h_m}{q_m}\right)\right| < rB_1^{1+3\delta}\, q_1^{-r_1(\gamma-\eta)\kappa} <$$

$$< B_1^{1+4\delta}\, q_1^{-r_1(\gamma-\eta)\kappa} <$$

$$< q_1^{(1+4\delta)\delta r_1 - r_1(\gamma-\eta)\kappa}.$$

將此與 (56) 比較,卽得

$$-m r_1(1+\delta) < (1+4\delta)\delta r_1 - r_1(\gamma-\eta)\kappa,$$

即

$$\kappa < \frac{m(1+\delta)+\delta(1+4\delta)}{\gamma-\eta} < \frac{m(1+4\delta)}{\gamma-\eta},$$

此與 (51) 相違. 定理 1 卽已證明.

§4. Roth 定理之應用.

定理 1. 設 $n \geqslant 3$,

$$f(x,y) = b_0 x^n + b_1 x^{n-1} y + \cdots + b_n y^n$$

爲一不可化齊次多項式,其係數爲有理整數. 又設

$$g(x,y) = \sum_{r+s \leqslant n-3} g_{rs} x^r y^s$$

爲一次數至多爲 $n-3$ 之有理係數多項式. 則不定方程

$$f(x,y) = g(x,y) \tag{1}$$

至多有有限對整數解 (x, y).

證: 我們祇須考慮

$$|x| \leqslant |y|$$

之情形 (對 $|x| > |y|$ 之情形,處理之方法相同). $y=0$ 之解至多爲 1. 故我們僅限於討論 $y>0$ 之解. 令 $\alpha_1, \cdots, \alpha_n$ 爲方程

$$f(x,1) = 0$$

之根, $G = \max(|g_{rs}|)$. 則由 (1), 卽得

$$|b_0(x-\alpha_1 y)\cdots(x-\alpha_n y)| \leqslant G(1+2y+\cdots+(n-2)y^{n-3}) \leqslant \leqslant n^2 G y^{n-3}. \tag{2}$$

故必有一 v 使

$$|x-\alpha_v y| < c_1 y^{1-\frac{3}{n}}$$

(c_1 及以下之 $c_2, \cdots, c_5$ 皆爲正常數).

因當 $\mu \neq v$, y 大於一適當大之 c_2 時,

$$|x-\alpha_\mu y| = |(\alpha_v-\alpha_\mu)y + (x-\alpha_v y)| > c_3 y - c_1 y^{1-\frac{3}{n}} > c_4 y, \tag{3}$$

故由 (2) 及 (3), 卽得

$$|x-\alpha_\nu y|<\frac{c_5}{y^2}$$

或

$$\left|\alpha_\nu-\frac{x}{y}\right|<\frac{c_5}{y^3}.$$

由定理 3.1, 此不等式僅有有限多組解; 若 $y\leqslant c_2$, 情形乃屬顯然. 定理卽得證明.

定理 2 (Thue). 設

$$g(x,y)=b_0x^n+b_1x^{n-1}y+\cdots+b_ny^n$$

爲一有理整係數之不可化齊次多項式, a 爲有理整數, 則

$$g(x,y)=a$$

僅有有限多組整數解.

證: 此乃上定理之一特別情形.

定理 3 (Thue). 上定理中如已假定 $a\neq 0$, 則可不必假定 $g(x,y)$ 爲不可化, 但須假定 $g(x,y)$ 非一次式之 n 方及二次式之 $\frac{n}{2}$ 方.

證: 若 $g(z)=g(z,1)$ 不可化, 固勿待論. 若 $g(z)$ 爲一 $m(\geqslant 3)$ 次不可化多項式 $h(z)$ 之乘方, 卽

$$g(z)=(h(z))^{n/m},$$

則問題一變而爲解方程 $y^m h\left(\frac{x}{y}\right)=a^{m/n}$. 若 $a^{m/n}$ 是一有理整數, 則問題化爲定理 2 之情形. 若 $a^{m/n}$ 非有理整數, 則此方程顯然無解. 今假定

$$g(z)=g_1(z)\,g_2(z),$$

$g_1(z)$ 與 $g_2(z)$ 分別爲 r 次與 s 次整係數多項式, 且其間無公因子. 如是, 所討論之問題一變而爲求解

$$y^r g_1\left(\frac{x}{y}\right)=a_1,\qquad y^s g_2\left(\frac{x}{y}\right)=a_2,\qquad a=a_1a_2.$$

已與 a, 則 a_1,a_2 僅有有限對. 若有一解 $y\neq 0,\pm 1$, 則

$$y^r g_1(z)=a_1,\qquad y^s g_2(z)=a_2$$

有公根, 卽

$$a_2^r\,(g_1(z))^s = a_1^s\,(g_2(z))^r.$$

但 $g_1(z)$ 與 $g_2(z)$ 無公因子，又 $g_2(z) \neq \pm a_2$, $g_1(z) \neq \pm a_1$，故此式不可能成立. $y = 0, \pm 1$ 之情況十分顯然，不贅.

附註: 定理中 $a \neq 0$ 乃一必要條件，蓋 $x^3 - y^3 = 0$ 有無限多組解. 又 $(sx + ty)^n = a^n$, $(x^2 - y^2)^l = a^l$ 皆有無限多組解，故其他條件亦不可少.

§5. Thue 定理之應用.

定理 1 (Landau-Ostrowski-Thue). 設 $n \geqslant 3$, $b^2 - 4ac \neq 0$, $a \neq 0$, $d \neq 0$. 則不定方程

$$ay^2 + by + c = dx^n \tag{1}$$

僅有有限個解.

證: 由 (1) 可知

$$(2ay+b)^2 - (b^2-4ac) = 4ad\,x^n.$$

若

$$y_1^2 - (b^2-4ac) = 4adx^n$$

僅有有限個解，則原式亦然. 因之，在今後之討論中，不妨假定 $a = 1$, $b = 0$. 卽祗需證明當 $n \geqslant 3$, $k \neq 0$, $l \neq 0$ 時，

$$y^2 - k = l\,x^n \tag{2}$$

僅有有限個解.

1) 設 k 爲平方數 m^2，則得

$$(y-m)\,(y+m) = l\,x^n.$$

當 $x = 0$ 時. $y = \pm m$. 今設 $x \neq 0$，此時 $y \neq \pm m$. 又因若 $p \nmid 2ml$，則 p 不能同時爲 $y + m$ 及 $y - m$ 的素因子. 故能將 $y + m$ 和 $y - m$ 表成如下形式:

$$y + m = \pm\, p_1^{r_1} \cdots p_j^{r_j}\, z^n = q\, z^n, \qquad 0 \leqslant r_i \leqslant n-1,$$

$$y - m = \pm\, p_1^{s_1} \cdots p_j^{s_j}\, w^n = t\, w^n, \qquad 0 \leqslant s_i \leqslant n-1,$$

其中 $p_1, \cdots, p_j$ 爲 $2ml$ 的素因子，因此 q 與 t 都祗能取有限個非零之值.

又對於一組 $q \neq 0$, $t \neq 0$, $f(z) = qz^n - t$ 無重根，故能適合定理 4.3 的條件. 因此不定方程

$$q z^n - t w^n = 2m$$

祗能有有限組非零解答. 定理得證.

2) 設 k 非平方數,命

$$\vartheta = \begin{cases} \sqrt{k}, & k > 0; \\ i\sqrt{|k|}, & k < 0. \end{cases}$$

今祗需研究 (2) 式中 $x > 0$ 之解,卽討論

$$y^2 - k = l x^n, \qquad x > 0 \tag{3}$$

的解. 命 x, y 爲 (3) 的任何一組解. 則由定理 6.10.5 可知有整數 r 及 q, 使

$$\left|\frac{y}{x} - \frac{r}{q}\right| < \frac{1}{q\sqrt{x}}, \qquad 0 < q \leqslant \sqrt{x}. \tag{4}$$

命

$$qy - rx = s,$$

則有

$$|s| < \sqrt{x} \tag{5}$$

及

$$s \equiv qy \pmod{x}. \tag{6}$$

又命

$$t = \left(\frac{s^2 - q^2 k}{x}\right)^n,$$

則因 k 非平方數,故 $t \neq 0$; 又由 (6) 及 (3) 可知:

$$s^2 - q^2 k \equiv q^2 (y^2 - k) \equiv q^2 l x^n \equiv 0 \pmod{x},$$

故 t 爲一整數. 又因

$$|t| \leqslant \left(\frac{s^2 + q^2 |k|}{x}\right)^n < \left(\frac{x + x|k|}{x}\right)^n = (1 + |k|)^n,$$

故對於給定的 n 及 k, 整數 t 祗能取有限個非零之値.

再命

$$\beta = \frac{(s - q\vartheta)^n (y + \vartheta)}{x^n}, \qquad \xi = s + q\vartheta,$$

則易見

$$t(y + \vartheta) = \beta \xi^n. \tag{7}$$

由於

$$(s-q\vartheta)^n=(q(y-\vartheta)-rx)^n=(A_1+A_2\vartheta)(y-\vartheta)+(-1)^n r^n x^n,$$

故得

$$x^n\beta=(s-q\vartheta)^n(y+\vartheta)=(A_1+A_2\vartheta)(y^2-k)+(-1)^n r^n x^n(y+\vartheta)=$$
$$=(A_1+A_2\vartheta)\,l\,x^n+(A_3+A_4\vartheta)\,x^n=(A_5+A_6\vartheta)\,x^n,$$

亦卽

$$\beta=A_5+A_6\vartheta, \tag{8}$$

其中 $A_1, A_2, \cdots, A_6$ 皆爲與 x,y 有關的整數.

因

$$|y|+|\vartheta|\leqslant\sqrt{|k|+|l|\,x^n}+\sqrt{|k|}\leqslant x^{n/2}(\sqrt{|k|+|l|}+\sqrt{|k|})$$

及

$$|s|+q|\vartheta|\leqslant\sqrt{x}+\sqrt{x}\sqrt{|k|}=\sqrt{x}\,(1+\sqrt{|k|}),$$

故得

$$|A_5\pm A_6\vartheta|=\left|\frac{(s\mp q\vartheta)^n(y\pm\vartheta)}{x^n}\right|\leqslant$$
$$\leqslant(1+\sqrt{|k|})^n(\sqrt{|k|+|l|}+\sqrt{|k|}).$$

於是由

$$A_5=\frac{1}{2}((A_5+A_6\vartheta)+(A_5-A_6\vartheta))$$

及

$$A_6=\frac{1}{2\vartheta}((A_5+A_6\vartheta)-(A_5-A_6\vartheta)),$$

可知對於給定的 n, k, l, 整數 A_5, A_6 祇能取有限個不同的值,亦卽 β 之個數有限. 又已知 t 之個數也有限,所以對於給定的 n, k, l, 祇有有限個方程 (7).

由 (7) 式得

$$t(y+\vartheta)=(A_5+A_6\vartheta)(s+q\vartheta)^n,$$

及

$$t(y-\vartheta)=(A_5-A_6\vartheta)(s-q\vartheta)^n.$$

於是

$$2t=\frac{1}{\vartheta}[(A_5+A_6\vartheta)(s+q\vartheta)^n-(A_5-A_6\vartheta)(s-q\vartheta)^n]. \tag{9}$$

當 $n, t(\neq 0)$, A_5, A_6 已與, 若能證明上式右邊爲一適合定理 4.3 假定的整係數多項式 $g(s,q)$,則 (9) 式祇能有有限組整數解 (s,q),於是再由 (7) 式,可知祇能有有限個不同的 y, 因之 (2) 式也祇能有有限組整數解 (x,y),而定理明矣.

欲證明 $g(s,q)$ 適合定理 4.3 的假定,祇須證明

$$f(z)=\frac{1}{\vartheta}\left[(A_5+A_6\vartheta)(z+\vartheta)^n-(A_5-A_6\vartheta)(z-\vartheta)^n\right]$$

無重根卽足. 但此爲顯然之事,蓋若不然,設

$$f(z)=0, \qquad f'(z)=0$$

有公共解 $z=z_0$, 則 z_0 必適合

$$\frac{A_5+A_6\vartheta}{A_5-A_6\vartheta}=\left(\frac{z_0-\vartheta}{z_0+\vartheta}\right)^n=\left(\frac{z_0-\vartheta}{z_0+\vartheta}\right)^{n-1},$$

因得 $\frac{z-\vartheta}{z+\vartheta}=1$, 此不可能. 故得定理.

習題 1. 設 n 爲一奇數 >1. 依次排列自然數之平方及 n 次方:

$$1=z_1<z_2<z_3<\cdots.$$

證明

$$z_{\nu+1}-z_\nu\to\infty.$$

習題 2. 命 $\langle\xi\rangle=\min(\xi-[\xi],[\xi]+1-\xi)$,則

$$\lim_{\substack{x\to\infty\\ x\text{ 非平方數}}} x^{n/2}\langle x^{n/2}\rangle=\infty.$$

§6. e 之超越性.

前已證明超越數之存在性,且實數中幾乎全部是超越數,蓋代數數集僅一可數集耳. 今轉而發問: 某一定數是否爲超越數, 如 e, π, $\sin 1$ 等是否爲超越數. 此種問題,遠較前之籠統的存在性爲難. 本節及下節中將證明 e, π 之超越性. 但迄今爲止數學家仍無人能證明 $e+\pi$ 爲超越數或否. 又如 Euler 常數

$$\gamma=\lim_{n\to\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}-\log n\right)$$

是否爲超越數亦爲一未能證明之難題. 不僅如此,且無人能證明 γ 爲無理數或否. 此乃著名之 Hilbert 第七問題之一部分,其另一部分將爲 §§8—10 論證之主題.

定理 1. e 非有理數.

證: 如能證明 e^{-1} 非有理數卽得定理. 命

$$e^{-1}=\sigma_n+\rho_n,$$

此處

$$\sigma_n=\sum_{k=0}^{n}\frac{(-1)^k}{k!},\qquad \rho_n=\sum_{k=n+1}^{\infty}\frac{(-1)^k}{k!}.$$

易見

$$0<(-1)^{n+1}\rho_n=\frac{1}{(n+1)!}-\frac{1}{(n+2)!}+\cdots<\frac{1}{(n+1)!},$$

因得

$$0<n!\,\rho_n(-1)^{n+1}<\frac{1}{n+1}<1,$$

卽

$$n!\,e^{-1}=n!\,\sigma_n+n!\,\rho_n(-1)^{n+1}$$

決不是一整數.

定理 2. 命

$$f(x)=\sum_{m=0}^{n}a_m x^m,$$

$$F(x)=\sum_{k=0}^{n}f^{(k)}(x),\qquad F(0)e^x-F(x)=Q(x),$$

則

$$|Q(x)|\leqslant e^{|x|}\sum_{m=0}^{n}|a_m|\,|x|^m.$$

證: 有恆等式

$$F(x)=\sum_{k=0}^{n}\sum_{m=k}^{n}a_m\frac{m!}{(m-k)!}x^{m-k}=$$

$$=\sum_{m=0}^{n}a_m\sum_{k=0}^{m}\frac{m!}{(m-k)!}x^{m-k}=\sum_{m=0}^{n}a_m\sum_{k=0}^{m}\frac{m!}{k!}x^k.$$

特别,有

$$F(0)=\sum_{m=0}^{n}a_m\,m!.$$

故

$$|Q(x)|=\left|\sum_{m=0}^{n}a_m\sum_{k=0}^{\infty}\frac{m!}{k!}x^k-\sum_{m=0}^{n}a_m\sum_{k=0}^{m}\frac{m!}{k!}x^k\right|=$$

$$=\left|\sum_{m=0}^{n}a_m\sum_{k=m+1}^{\infty}\frac{m!}{k!}x^k\right|\leqslant$$

$$\leqslant\sum_{m=0}^{n}|a_m|\sum_{k=m+1}^{\infty}|x|^k/(k-m)!=$$

$$=\sum_{m=0}^{n}|a_m|\,|x|^m\sum_{l=1}^{\infty}\frac{|x|^l}{l!}\leqslant e^{|x|}\sum_{m=0}^{n}|a_m|\,|x|^m.$$

定理 3 (Hermite). e 是超越數.

證: 假定 e 適合於 $P(x)$, 而

$$P(x)=\sum_{h=0}^{m} g_h x^h, \qquad g_0\neq 0, \quad m>0,$$

此處 g_h 是有理整數. 命 p 爲一素數 $>\max(m, |g_0|)$. 又命

$$f(x)=\frac{x^{p-1}\prod_{h=1}^{m}(h-x)^p}{(p-1)!}=\sum_{k=0}^{n} a_k x^k \qquad (a_k=a_k(p)).$$

由於 h 是 $f(x)=0$ 之 p 重根,故可書爲

$$f(x)=\frac{(m!)^p x^{p-1}+A_p x^p+\cdots}{(p-1)!}=$$

$$=\frac{B_{p,h}(x-h)^p+B_{p+1,h}(x-h)^{p+1}+\cdots}{(p-1)!},$$

此處 A,B 皆爲有理整數. 由此 $f(x)$ 做出定理 2 中之 $F(x)$ 及 $Q(x)$. 則

$$0=F(0)P(e)=F(0)\sum_{h=0}^{m} g_h e^h=$$

$$=\sum_{h=0}^{m} g_h F(h)+\sum_{h=0}^{m} g_h Q(h). \tag{1}$$

又已知

$$\sum_{h=0}^{m} g_h F(h)=g_0\sum_{k=0}^{n} f^{(k)}(0)+\sum_{h=1}^{m} g_h \sum_{k=0}^{n} f^{(k)}(h)=$$

$$=g_0((m!)^p+pA_p+\cdots)+\sum_{h=1}^{m} g_h(pB_{p,h}+p(p+1)B_{p+1,h}+\cdots),$$

此乃一有理整數. 於上式右邊 $p\nmid g_0(m!)^p$, 而其餘各項皆爲 p 之倍數,故

$$\left|\sum_{h=0}^{m} g_h F(h)\right|\geqslant 1.$$

若能證明,有一素數 $p>\max(m, |g_0|)$,使

$$\left|\sum_{h=0}^{m} g_h Q(h)\right|<1,$$

則由 (1) 式引出矛盾. 由定理 2 可知祗需證明,對一固定的 x, 當 $p\to\infty$ 時

$$\sum_{k=0}^{n} |a_k|\ |x|^k\to 0$$

卽足. 此點之證明極易:

$$\sum_{k=0}^{n} |a_k|\ |x|^k \leqslant \frac{|x|^{p-1} \prod_{h=1}^{m} (h+|x|)^p}{(p-1)!} \to 0.$$

§7. π 之超越性.

定理 1. π 非有理數.

證: 若 $\pi = \frac{a}{b}$, a 和 b (>0) 是有理整數,命

$$f(x) = \frac{x^n (a-bx)^n}{n!}$$

及

$$F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - \cdots + (-1)^n f^{(2n)}(x),$$

易見 $f(x)$ 及其導數當 $x = 0$ 及 π 時取整數值,卽 $F(0)$ 及 $F(\pi)$ 是整數. 今

$$\frac{d}{dx}(F'(x) \sin x - F(x) \cos x) = (F''(x) + F(x)) \sin x = f(x) \sin x,$$

故得

$$\int_0^{\pi} f(x) \sin x\, dx = F(\pi) - F(0) \tag{1}$$

是一整數.

但當 $0 < x < \pi$ 及 n 充分大時,有

$$0 < f(x) \sin x < \frac{\pi^n a^n}{n!} < \frac{1}{\pi},$$

故得

$$0 < \int_0^{\pi} f(x) \sin x\, dx < 1. \tag{2}$$

(2) 與 (1) 矛盾,故得定理.

定理 2 (Lindemann). π 是超越數.

證: 由於 i 是代數數,又由於二代數數之積及商仍爲代數數,可知 π 與 $i\pi$ 或同時是代數數,或同時非代數數. 故祗需證明 $i\pi$ 非代數數卽足.

假定 $i\pi$ 適合於

$$f(x) = a x^m + a_1 x^{m-1} + \cdots = 0, \quad a > 0,$$

則 $ai\pi$ 適合於

$$a^{m-1} f\left(\frac{x}{a}\right) = x^m + a_1 x^{m-1} + \cdots = 0.$$

又因爲 $i\pi$ 與 $ai\pi$ 同爲代數數或否,今祗需證明 $ai\pi$ 適合

$$P(y) = y^m + k_{m-1} y^{m-1} + \cdots + k_0 = 0, \qquad m > 0$$

爲不可能.

命

$$P(y) = \prod_{h=1}^{m} (y - a\,\alpha_h).$$

因爲 $1 + e^{i\pi} = 0$, 故祇需證明

$$R = \prod_{h=1}^{m} (e^0 + e^{\alpha_h}) \neq 0.$$

R 可以寫成

$$R = c + \sum e^{\alpha} + \sum e^{\alpha+\alpha'} + \cdots =$$

$$= c + e^{\beta_1} + e^{\beta_2} + \cdots + e^{\beta_r},$$

於此, c 爲 2^m 項中指數之和爲零者之個數,而 $\beta_1, \cdots, \beta_r$ 不爲零。

命 p 爲一素數 $> \max\left(c,\ a,\ \prod_{h=1}^{r} a|\beta_h|\right)$. 命

$$f(x) = \frac{(ax)^{p-1} \prod_{h=1}^{r} (ax - a\,\beta_h)^p}{(p-1)!} = \sum_{k=0}^{n} a_k x^k.$$

與定理 6.3 之證明相似,可得

$$f(x) = \frac{A_{p-1} x^{p-1} + A_p x^p + \cdots}{(p-1)!} =$$

$$= \frac{\gamma_{p,h} (x - \beta_h)^p + \gamma_{p+1,h} (x - \beta_h)^{p+1} + \cdots}{(p-1)!},$$

式中諸 A 爲 $a\,\beta_1, \cdots, a\,\beta_r$ 之對稱函數, 故亦爲 $a\,\alpha_1, \cdots, a\,\alpha_h$ 之對稱函數, 故爲有理整數,且 $A_{p-1} \not\equiv 0 \pmod p$.

做對應之 $F(x)$ 及 $Q(x)$,則

$$F(0)\,R = F(0)\left(c + \sum_{h=1}^{r} e^{\beta_h}\right) = c\,F(0) + \sum_{h=1}^{r} F(\beta_h) + \sum_{h=1}^{r} Q(\beta_h),$$

於此,

$$c\,F(0) = c\,(A_{p-1} + p\,A_p + \cdots)$$

爲一有理整數,但非 p 之倍數. 又

$$\sum_{h=1}^{r} F(\beta_h) = \sum_{h=1}^{r} (p\,\gamma_{p,h} + p(p+1)\,\gamma_{p+1,h} + \cdots) =$$

$$=p\sum_{h=1}^{r}\gamma_{p,h}+p(p+1)\sum_{h=1}^{r}\gamma_{p+1,h}+\cdots=$$
$$=p\,c_p+p(p+1)\,c_{p+1}+\cdots,$$

$c_p, c_{p+1}, \cdots$ 爲 $a\beta_1, \cdots, a\beta_r$ 之對稱函數，故爲有理整數. 故 $\sum_{h=1}^{r}F(\beta_h)$ 爲 p 之倍數. 因而

$$\left|c\,F(0)+\sum_{h=1}^{r}F(\beta_h)\right|\geqslant 1.$$

今祇需證明，當 p 充分大時

$$\left|\sum_{h=1}^{r}Q(\beta_h)\right|<1,$$

卽當 x 固定時

$$\lim_{p\to\infty}\sum_{k=1}^{n}|a_k|\,|x|^k=0.$$

由於當 $p\to\infty$ 時

$$\sum_{k=1}^{n}|a_k|\,|x|^k\leqslant\frac{(a|x|)^{p-1}\prod_{h=1}^{r}(a|x|+a|\beta_h|)^p}{(p-1)!}\to 0.$$

故得定理.

附註：此定理也回答了祇用圓規直尺不能“化圓爲方”的問題. 卽不能用圓規及直尺作一線段其長等於單位圓之弧長之問題.

習題 1. 若 ξ 是有理數，則 $\sinh\xi$ 是超越數.

習題 2. 證明 e^i 是超越數. 因之證明 $\sin 1$ 是超越數.

§ 8. Hilbert 第七問題.

在 1900 年 Hilbert 曾列舉 23 個數學上未解決之問題. 其中之第七問題（除已見於 §6 之一部分外）爲：

若 α 是一代數數 $\neq 0, 1$，又 β 是一非有理數之代數數，問 α^β 是否是超越數. 他並舉出兩例：卽能否證明 $2^{\sqrt{2}}$ 及 $e^\pi=(-1)^{-i}$ 是超越數.

關於此一問題之第一個重要貢獻是在 1929 年由蘇聯數學家 A. O. Гельфонд 所給出. 彼證明 e^π 是超越數，並指出其方法可以解決 β 在任意虛二次域中之 Hilbert 問題. 1930 年 Кузьмин 將 Гельфонд 之方法推到實二次域. 特別證明了 $2^{\sqrt{2}}$ 是超越數.

在 1934 年 Гельфонд 完整地解決了 Hilbert 問題 (1935 年 Schneider 給與另一證明). Гельфонд 的方法用到複變函數論,但其方法創造了代數與分析統一運用的一個美好範例.

在 Hilbert 敘述此問題時,曾經提起,此問題之解決將後於 Riemann 推測及 Fermat 問題. 但今天事實已説明適得其反. 因之,在一問題未解決以前,實難以推測其難易也.

習知當 $0 < p < q$ 時, q 個未知數 $x_1, \cdots, x_q$ 的 p 個齊次線性聯立方程必有一非全爲零之解. 且如其係數爲有理整數,則亦有非全爲零的有理整數解. 今往證明, 當 $|x_1|, \cdots, |x_q|$ 受某種限制時, 該方程組仍有非全爲零的有理整數解.

引 1. 若 $0 < p < q$, a_{kl} 爲有理整數, 且 $|a_{kl}| \leqslant A$ $(A \geqslant 1)$, 則有一組非全爲零的有理整數 $x_1, \cdots, x_q$ 適合於

$$a_{k1}x_1 + \cdots + a_{kq}x_q = 0, \qquad 1 \leqslant k \leqslant p \tag{1}$$

及

$$|x_l| < 1 + (qA)^{p/(q-p)}, \qquad 1 \leqslant l \leqslant q. \tag{2}$$

證: 先討論變形

$$y_k = a_{k1}x_1 + \cdots + a_{kq}x_q, \qquad 1 \leqslant k \leqslant p. \tag{3}$$

此變形變有理整數組 $(x_1, \cdots, x_q)$ 爲有理整數組 $(y_1, \cdots, y_p)$. 命 H 爲一自然數. 若

$$|x_l| \leqslant H, \qquad 1 \leqslant l \leqslant q, \tag{4}$$

則

$$|y_k| \leqslant |a_{k1}|\,|x_1| + \cdots + |a_{kq}|\,|x_q| \leqslant qAH, \qquad 1 \leqslant k \leqslant p. \tag{5}$$

適合於 (4) 之 $(x_1, \cdots, x_q)$ 共有 $(2H+1)^q$ 組,而適合於 (5) 之 $(y_1, \cdots, y_p)$ 共有 $(2qAH+1)^p$ 組,故若

$$(2H+1)^q > (2qAH+1)^p, \tag{6}$$

則至少有一組 $(y_1, \cdots, y_p)$ 對應於兩組不同的數 $(x'_1, \cdots, x'_q)$ 及 $(x''_1, \cdots, x''_q)$. 故 $x_1 = x'_1 - x''_1, \cdots, x_q = x'_q - x''_q$ 適合於 (1) 式,且

$$|x_l| \leqslant 2H. \tag{7}$$

取偶數 $2H$ 適合於

$$(qA)^{p/(q-p)} - 1 \leqslant 2H < (qA)^{p/(q-p)} + 1. \tag{8}$$

由於此不等式兩端之距離爲 2，故此種選擇一定可能．在此選擇下，

$$(2qAH+1)^p < (qA)^p(2H+1)^p \leqslant (2H+1)^{q-p}(2H+1)^p = (2H+1)^q,$$

卽適合 (6) 式．故由 (7)，(8) 二式得出本引．

此引可以推廣到代數數之範圍（卽引 3）．命 K 表一 h 次之代數數域．且命 $\beta_1, \cdots, \beta_h$ 爲其一整底，卽任一 K 中之整數可以唯一地表成爲 $a_1\beta_1+\cdots+a_h\beta_h$ 之形式，其中 $a_1, \cdots, a_h$ 爲有理整數．用符號 $\overline{|\alpha|}$ 表示 α 之諸共軛數 $\alpha^{(i)}$ $(1\leqslant i\leqslant h)$ 之絕對值之最大值，卽

$$\overline{|\alpha|} = \max_{1\leqslant i\leqslant h}(|\alpha^{(i)}|).$$

引 2. 若 α 爲一代數整數

$$\alpha = a_1\beta_1+\cdots+a_h\beta_h,$$

則

$$|a_h| \leqslant c\overline{|\alpha|},$$

此處 c（及今後之 c_1, c_2）爲僅與 K 及所選定之整底 $\beta_1, \cdots, \beta_h$ 有關的自然數．

此引可由解聯立方程組

$$\alpha^{(i)} = a_1\beta_1^{(i)}+\cdots+a_h\beta_h^{(i)}, \qquad 1\leqslant i\leqslant h$$

得之．

引 3. 若 $0<p<q$，α_{kl} $(1\leqslant k\leqslant p,\ 1\leqslant l\leqslant q)$ 爲 K 中之整數，且 $\overline{|\alpha_{kl}|}\leqslant A$，則有一組 K 中的非全爲零的代數整數 $\xi_1, \cdots, \xi_q$ 適合於

$$\alpha_{k1}\xi_1+\cdots+\alpha_{kq}\xi_q = 0, \qquad 1\leqslant k\leqslant p \tag{9}$$

及

$$\overline{|\xi_l|} < c_1(1+(c_1qA)^{p/(q-p)}), \qquad 1\leqslant l\leqslant q. \tag{10}$$

證：命

$$\xi_l = x_{l1}\beta_1+\cdots+x_{lh}\beta_h, \qquad 1\leqslant l\leqslant q,$$

此處 $x_{l1}, \cdots, x_{lh}$ 是有理整數．命

$$\alpha_{kl}\beta_r = a_{klr1}\beta_1+\cdots+a_{klrh}\beta_h, \tag{11}$$

此處 $a_{klr1}, \cdots, a_{klrh}$ 也是有理整數．於是 (9) 式變爲

$$0 = \sum_{l=1}^{q}\alpha_{kl}\xi_l = \sum_{l=1}^{q}\alpha_{kl}\sum_{r=1}^{h}x_{lr}\beta_r =$$

$$= \sum_{r=1}^{h}\sum_{l=1}^{q}x_{lr}\sum_{u=1}^{h}a_{klru}\beta_u =$$

$$= \sum_{u=1}^{h} \left(\sum_{r=1}^{h} \sum_{l=1}^{q} a_{klru} x_{lr} \right) \beta_u, \qquad 1 \leqslant k \leqslant p.$$

由於 $\beta_1, \cdots, \beta_h$ 是線性獨立的,故得由 hp 個方程所成的方程組

$$\sum_{r=1}^{h} \sum_{l=1}^{q} a_{klru} x_{lr} = 0, \qquad 1 \leqslant u \leqslant h, \qquad 1 \leqslant k \leqslant p, \tag{12}$$

其中有 hq 個未知數.

由 (11) 及引 2, 可知 $|a_{klru}| \leqslant \max_{1 \leqslant i \leqslant h} \overline{|\beta_i|}\, A \leqslant c_2 A$.

故由引 1 可知 (12) 式有非皆爲零之有理整數解答,且適合於

$$|x_{lr}| \leqslant 1 + (hq\, c_2 A)^{p/(q-p)}, \qquad 1 \leqslant l \leqslant q, \qquad 1 \leqslant r \leqslant h.$$

故得

$$\overline{|\xi_l|} \leqslant |x_{l1}|\, \overline{|\beta_1|} + \cdots + |x_{lh}|\, \overline{|\beta_h|} \leqslant$$
$$\leqslant c_2 h\, (1 + (hq\, c_2 A)^{p/(q-p)}).$$

命 $c_2 h = c_1$, 卽得引理.

§ 9. Гельфонд 之證明.

設 $\alpha \neq 0,1$ 是一代數數,又 β 是一非有理數之代數數,要證明 α^β 是超越數. 若不然,卽若 $\gamma = \alpha^\beta = e^{\beta \log \alpha}$ (此處 $\log \alpha$ 取 α 之對數中任意固定的一值, 且 $\log \alpha \neq 0$) 也是代數數,則可導出矛盾.

設 α, β, γ 皆在一 h 次之代數數域 K 中. 命

$$m = 2h + 2, \qquad n = \frac{q^2}{2m},$$

此處 $q^2 = t$ 乃一自然數之平方且爲 $2m$ 之倍數者. 又命 $\rho_1, \rho_2, \cdots, \rho_t$ 代表 t 個數

$$(a + b\beta) \log \alpha, \qquad 1 \leqslant a \leqslant q, \qquad 1 \leqslant b \leqslant q.$$

引進整函數

$$R(x) = \eta_1 e^{\rho_1 x} + \cdots + \eta_t e^{\rho_t x}, \tag{1}$$

於此 $\eta_1, \cdots, \eta_t$ 爲待定係數. 今由下面的條件來定出 $\eta_1, \cdots, \eta_t$. 卽解有 $t = 2mn$ 個未知數 $\eta_1, \cdots, \eta_t$ 的 mn 個齊次線性聯立方程組

$$(\log \alpha)^{-k} R^{(k)}(l) = 0, \qquad 0 \leqslant k \leqslant n-1, \qquad 1 \leqslant l \leqslant m. \tag{2}$$

此方程組的係數在 K 中,且其係數是

$$(\log\alpha)^{-k}((a+b\beta)\log\alpha)^k e^{l(a+b\beta)\log\alpha}=(a+b\beta)^k\alpha^{al}\gamma^{bl},$$

$$1\leqslant l\leqslant m,\qquad 1\leqslant a,\ b\leqslant q,\qquad 0\leqslant k\leqslant n-1.$$

習知有一自然數 c_1（此處 c_1 及以後之 $c_2, c_3, \cdots$ 皆表與 n 無關之自然數）存在，使 $c_1\alpha, c_1\beta, c_1\gamma$ 皆爲 K 中之整數．故於該方程組之每一係數乘以

$$c_1^{n-1}\,c_1^{mq}\,c_1^{mq}=c_1^{n-1+2mq}\ (\leqslant c_2^n)$$

後，其係數皆變成 K 中之整數．且其諸係數之共軛數之絕對值皆

$$\leqslant c_2^n(q+q\,\overline{|\beta|})^{n-1}\,\overline{|\alpha|}^{mq}\,\overline{|\gamma|}^{mq}\leqslant c_3^n\,n^{\frac{1}{2}(n-1)}.$$

故由引 8.3 知有一組非全爲零的 K 中之整數 $\eta_1, \cdots, \eta_t$ 爲其解，且

$$\overline{|\eta_k|}\leqslant c_4^n\,n^{\frac{1}{2}(n+1)},\qquad 1\leqslant k\leqslant t.$$

因爲 $\rho_1, \cdots, \rho_t$ 各不相同，可知 $R(x)$ 不恆等於零．不然，展開 (1) 式右邊可得

$$\eta_1\rho_1^k+\eta_2\rho_2^k+\cdots+\eta_t\rho_t^k=0,\qquad k=0,1,2,\cdots$$

由此得出 $\eta_1=\eta_2=\cdots=\eta_t=0$，此乃矛盾．於是由 (2) 可知

$$R(x)=a_{n,l}(x-l)^n+a_{n+1,l}(x-l)^{n+1}+\cdots,\qquad 1\leqslant l\leqslant m,\tag{3}$$

其中 $a_{n,l}, a_{n+1,l}, \cdots$ 不全爲零．故必有一自然數 r 存在，使

$$R^{(k)}(l)=0,\qquad 0\leqslant k\leqslant r-1,\qquad 1\leqslant l\leqslant m,$$

但對某一 $l_0(1\leqslant l_0\leqslant m)$，

$$R^{(r)}(l_0)\neq 0.$$

由 (3)，顯然 $r\geqslant n$.

今往研究數

$$(\log\alpha)^{-r}R^{(r)}(l_0)=\rho\neq 0.\tag{4}$$

此數在 K 中，且 $c_1^{r+2mq}\rho$ 是 K 中之整數，故

$$|N(\rho)|>c_1^{-h(r+2mq)}>c_5^{-r}.\tag{5}$$

另一方面，

$$\overline{|\rho|}\leqslant t\,c_4^n\,n^{\frac{1}{2}(n+1)}(c_6\,q)^r\,c_7^q\leqslant c_8^r r^{r+\frac{3}{8}}.\tag{6}$$

今往求出 $|\rho|$ 之一適當上界．用 Cauchy 積分公式於整函數

$$S(z)=r!\,\frac{R(z)}{(z-l_0)^r}\prod_{\substack{k=1\\k\neq l_0}}^{m}\left(\frac{l_0-k}{z-k}\right)^r.$$

則有

$$\rho=(\log\alpha)^{-r}S(l_0)=(\log\alpha)^{-r}\frac{1}{2\pi i}\int_C\frac{S(z)}{z-l_0}\,dz, \tag{7}$$

此處 C 乃圓

$$|z|=m\left(1+\frac{r}{q}\right),$$

故 l_0 $(\leqslant m)$ 在 C 中. 當 z 在圓周上變動時,有

$$|R(z)|\leqslant t\max_{1\leqslant k\leqslant t}|\eta_k|\,e^{(q+q|\beta|)\log|\alpha|\cdot m\left(1+\frac{r}{q}\right)}\leqslant t\,c_4^n\,n^{\frac12(n+1)}\,c_9^{r+q}\leqslant c_{10}^r\,r^{\frac12(r+3)},$$

$$|z-l_0|\geqslant|z|-|l_0|\geqslant m\left(1+\frac{r}{q}\right)-m=\frac{mr}{q},$$

$$|z-k|\geqslant\frac{mr}{q},\qquad 1\leqslant k\leqslant m,$$

$$\left|(z-l_0)^{-r}\prod_{\substack{k=1\\k\neq l_0}}^{m}\left(\frac{l_0-k}{z-k}\right)^r\right|\leqslant c_{11}^r\left(\frac{q}{r}\right)^{mr},$$

$$|S(z)|\leqslant r!\,c_{10}^r\,r^{\frac12(r+3)}\,c_{11}^r\left(\frac{q}{r}\right)^{mr}\leqslant c_{12}^r\,r^{\frac12 r(3-m)+\frac32},$$

故由 (7) 得

$$|\rho|\leqslant\frac{1}{2\pi}\,|(\log\alpha)^{-r}|\int_C\left|\frac{S(z)}{z-l_0}\right||dz|\leqslant$$

$$\leqslant|(\log\alpha)^{-r}|\cdot m\left(1+\frac{r}{q}\right)\cdot c_{12}^r\,r^{\frac12 r(3-m)+\frac32}\cdot\frac{q}{mr}\leqslant c_{13}^r\,r^{\frac12 r(3-m)+\frac32}. \tag{8}$$

由 (6) 及 (8),得

$$|N(\rho)|\leqslant c_{14}^r\,r^{(h-1)\left(r+\frac32\right)+\frac12(3-m)r+\frac32}.$$

以 $m=2h+2$ 代入後,即得

$$|N(\rho)|\leqslant c_{14}^r\,r^{-\frac12 r+\frac32 h}. \tag{9}$$

比較 (5) 式與 (9) 式,可得

$$r^{\frac12 r-\frac32 h}<c_{14}^r\,c_5^r=c_{15}^r.$$

當 n 充分大時,由於 $r\geqslant n$, 上式不可能,故得矛盾.

第十八章

Waring 問題及 Prouhet-Tarry 問題

§1. 引言. 1770 年 Waring 於 Meditationes Algebraicae 上曾作如次之推測:

凡正整數必為四個平方數之和,九個立方數之和,十九個四方數之和等等.

窺其詞意似謂:"有一整數 $s(k)$ 存在,每個正整數必為 $s(k)$ 個 k 乘方數之和."

待百餘年後, Hilbert 首先證明此言.

切實言之,以上之問題可以改述為: 命 k 是一固定的正整數. 問是否有一整數 $s=s(k)$,使對任一 $n(>0)$,不定方程

$$n=x_1^k+\cdots+x_s^k,\quad x_\nu\geqslant 0 \tag{1}$$

常有解答.

今以 $g(k)$ 表最小之 s 之具有此性質者. 故 Waring 之敍述乃

$$\text{“}g(2)=4,\quad g(3)=9,\quad g(4)=19\ \text{等等”}.$$

今以 $G(k)$ 表示凡充分大之整數 n 皆可以表為 $G(k)$ 個 k 乘方之和者. 卽若 $s\geqslant G(k)$,則 (1) 當 n 充分大時有解. 顯然

$$G(k)\leqslant g(k).$$

實際上兩者之間相差極遠.

在本章中僅證明一些極個別之結果. 而 Waring-Hilbert 定理 (卽 $g(k)<<\infty$) 將於次章中證明之. 該證明並非 Hilbert 原證,乃 Линник 所發明者,遠簡於 Hilbert 原證. Хинчин 稱之為數論三珠之一.

§2. $g(k)$ 及 $G(k)$ 之下限.

定理 1. $g(k)\geqslant 2^k+\left[\left(\frac{3}{2}\right)^k\right]-2.$

證: 命 $q=\left[\left(\frac{3}{2}\right)^k\right]$. 取

$$n=2^k q-1<3^k,$$

則此數祇能爲若干個 1^k 及 2^k 之和. 而 s 最小之分裂法爲

$$n=(q-1)2^k+(2^k-1)\cdot 1^k,$$

卽爲 $q-1$ 個 2^k 及 2^k-1 個 1^k 之和. 故

$$g(k)\geqslant 2^k+q-2.$$

由此立見

$$g(2)\geqslant 4,\quad g(3)\geqslant 9,\quad g(4)\geqslant 19,\quad g(5)\geqslant 37,\cdots.$$

Виноградов 氏引進了新方法,由該方法十分精確地估計了 $G(k)$ 的上限. Dickson, Pillai, Niven 經過 Виноградов 方法的實際計算, 因而肯定了

$$g(k)=2^k+\left[\left(\frac{3}{2}\right)^k\right]-2\qquad (k\neq 4,5).$$

對其他二種情況已知的結果爲

$$19\leqslant g(4)\leqslant 35,\qquad 37\leqslant g(5)\leqslant 54.$$

定理 2. 若 $k\geqslant 2$, 則 $G(k)\geqslant k+1$.

證: 命 $A(N)$ 爲不大於 N 之正整數之可以表爲

$$x_1^k+\cdots+x_k^k,\qquad x_\nu\geqslant 0$$

之形式者之個數,今排列 $x_1,\cdots,x_k$ 爲

$$0\leqslant x_1\leqslant x_2\leqslant\cdots\leqslant x_k\leqslant [N^{1/k}].$$

$A(N)$ 當不超過適合此諸不等式之整數數,卽

$$A(N)\leqslant \sum_{x_k=0}^{[N^{1/k}]}\ \sum_{x_{k-1}=0}^{x_k}\ \sum_{x_{k-2}=0}^{x_{k-1}}\cdots\sum_{x_1=0}^{x_2}1.$$

右邊之和爲

$$B(N)=\frac{1}{k!}([N^{1/k}]+1)([N^{1/k}]+2)\cdots([N^{1/k}]+k).$$

今用歸納法證明此點. 當 $k=1$, 此乃顯然. 故所待證者乃

$$\sum_{x=0}^{y}\binom{x+k-1}{k-1}=\binom{y+k}{k}.$$

而此式乃易證之式也.

當 $N\to\infty$

$$B(N)\sim\frac{N}{k!}<\frac{2}{3}N,$$

即當 N 充分大時

$$A(N)<\frac{2}{3}N.$$

因之,$A(N)$ 個數中不能包有小於 N 之全部正整數. 故

$$G(k)\geqslant k+1.$$

通過同餘式之討論還可以稍稍提高 $G(k)$ 之下限. 例如: 由於

$$x^4\equiv 0 \quad 或 \quad 1 \pmod{16},$$

故形如 $16m+15$ 之數至少要 15 個四乘方之和. 故得

$$G(4)\geqslant 15.$$

但若

$$16\cdot n=x_1^4+\cdots+x_{15}^4,$$

則得 $2\mid(x_1,\cdots,x_{15})$,即

$$n=x_1^4+\cdots+x_{15}^4.$$

又 31 不能表爲少於 16 個四次方之和,故 $16\cdot 31$ 必不能表爲 15 個四次方之和. 故得

$$G(4)\geqslant 16.$$

一般言之,此法可以證明:

定理 3. 若 $k=2^\theta\geqslant 4$, 則 $G(k)\geqslant 4k$.

證: 前已證明 $\theta=2$ 之情形. 今設 $\theta>2$. 不難證明

$$x^k\equiv 0 \quad 或 \quad 1 \pmod{4k}.$$

命 n 爲一奇數,若 $2^{\theta+2}n$ 可以表爲不多於 $2^{\theta+2}-1$ 個 k 乘方之和,則其中每一 k 乘方必爲偶數,即爲 2^k 之倍數,由於 $2^k>2^{\theta+2}$, 而 $2\nmid n$. 此不可能. 故得定理.

§3. Cauchy 定理.

命 $q>1$. 在本節中,我們將討論同餘式

$$x_1^k+\cdots+x_s^k\equiv n \pmod{q}$$

之可解條件. 由孫子定理可知,吾人僅須研究同餘式

$$x_1^k + \cdots + x_s^k \equiv n \pmod{p^l} \tag{1}$$

之可解條件卽可,此處 p 爲一素數. 因 $n = n - 1 + 1^k$, 故在下面的證明中我們常假定 $p \nmid n$.

在研究此問題之先,我們先來證明次之定理:

定理 1 (Cauchy). 設 $x_1, \cdots, x_m$ 代表 m 個互不同餘的數 $\bmod q$; $y_1, \cdots, y_n$ 代表 n 個互不同餘的數 $\bmod q$; 且存在一數 y_i 使當 $i \neq j$ 時, $(y_i - y_j, q) = 1$, 則 $x_u + y_v$ $(1 \leqslant u \leqslant m,\ 1 \leqslant v \leqslant n)$ 所代表的互不同餘 $\bmod q$ 的整數個數 $\geqslant \min(m + n - 1, q)$.

證: 當 $n = 1$, 定理顯然成立. 今設 $n \geqslant 2$, 並不妨假定定理中之 $i = 1$.

命 $z_1, \cdots, z_t$ 爲形如 $x_i + y_j$ 的互不同餘的數 $\bmod q$, 若 $t = q$, 則定理已經成立,故假定 $t < q$, 並以 X, Y, Z 分別記集合 $x_1, \cdots, x_m$; $y_1, \cdots, y_n$; $z_1, \cdots, z_t$.

作 $x_1 + y_1 + \lambda(y_n - y_1)$, 則當 $\lambda = 0, 1$ 時,此皆屬於 Z. 因 $(q, y_n - y_1) = 1$, 故必存在 λ_0 使 $x_1 + y_1 + (\lambda_0 - 1)(y_n - y_1) \in Z$ 而 $x_1 + y_1 + \lambda_0(y_n - y_1) \notin Z$, 命 $x_1 + y_1 + \lambda_0(y_n - y_1) + y_1 = \delta$, 則得 $\delta - y_1 \notin Z$ 而 $\delta - y_n \in Z$. 將 $y_1, \cdots, y_n$ 適當的加以排列,可得

$$\begin{cases} \delta - y_s \notin Z & (1 \leqslant s \leqslant r), \\ \delta - y_{s'} \in Z & (r < s' \leqslant n). \end{cases}$$

顯然 $r \leqslant n - 1$. 作 Z': $z = x_u + y_s$, $u = 1, 2, \cdots, m$, $s = 1, 2, \cdots, r$. 則 $\delta - y_{s'} \notin Z'$, 否則由 $\delta - y_{s'} = x_u + y_s$ 卽得 $\delta - y_s = x_u + y_{s'} \in Z$. 若 Z' 所代表的互不同餘 $\bmod q$ 的數的數目爲 t', 則 $t' \leqslant t - (n - r)$. 另一方面,由歸納法假定可知 $t' \geqslant m + r - 1$, 故得 $t \geqslant m + n - 1$.

定義. 設 $p^\tau \| k$, 則定義

$$\gamma = \begin{cases} \tau + 1, & 當\ p > 2; \\ \tau + 2, & 當\ p = 2. \end{cases}$$

定理 2. 若同餘式

$$x^k \equiv a \pmod{p^\gamma},\quad p \nmid a \tag{2}$$

有解,則當 $l > \gamma$ 時

$$x^k \equiv a \pmod{p^l}$$

亦有解.

證: 設 y 爲(2)之一解. g 爲 p^l 之一原根 (若 $p=2$, 可取 $g=5$). 決定整數 $b \geqslant 0$, 使

$$a \equiv y^k g^b \pmod{p^l}, \tag{3}$$

由此顯然即得 $g^b \equiv 1 \pmod{p^\gamma}$. 因之 $p^\tau(p-1) \mid b$. 令 $b = p^\tau(p-1)\, b_1$. 我們顯然可將 (3) 中之指數 b 代以

$$b + h\, p^{l-1}(p-1) = p^\tau(p-1)\,(b_1 + h\, p^{l-\tau-1}),$$

此處 h 爲任一整數. 命 $k = p^\tau k_1$, $(k_1, p) = 1$, 則可取 h 使

$$b_1 + h\, p^{l-\tau-1} \equiv 0 \pmod{k_1}.$$

由是即得

$$a \equiv y^k g^b \equiv y^k g^{b+h\, p^{l-1}(p-1)} \equiv y^k g^{h_1 k} \pmod{p^l}.$$

定理即已證明.

定理 3. 若 (1) 式對 $l=\gamma$ 有解,則對 $l>\gamma$ 亦有解.

證: 由假定,有 $y_1, \cdots, y_s$ 使

$$y_1^k + \cdots + y_s^k \equiv n \pmod{p^\gamma}.$$

因 $p \nmid n$, 故必有一 y, 不妨設爲 y_1, 使 $p \nmid y_1$, 由是即得

$$y_1^k \equiv n - y_2^k - \cdots - y_s^k \pmod{p^\gamma}.$$

由定理 2 有 x_1, 使

$$x_1^k + y_2^k + \cdots + y_s^k \equiv n \pmod{p^l}.$$

定理 4. 若 $k = 2^\tau$, 則當 $s \geqslant 4k$ 時, (1) 式常有解; 若 $k \neq 2^\tau$, 則當 $s \geqslant 3k+1$ 時, (1) 式常有解.

證: 我們顯然只須討論 $l \geqslant \gamma$ 時之情形. 由定理 3, 我們只須討論 $l=\gamma$ 之情形即可.

1) 若 $k = 2^\tau$, 則 $p^\gamma = 2^{\tau+2} = 4k$. 同餘式

$$x_1^k + \cdots + x_s^k \equiv n \pmod{2^\gamma}$$

當 $s \geqslant 4k$ 時顯然有解.

2_1) $p=2$, $k = 2^\tau k_0$, $k_0 > 1$, $2 \nmid k_0$. 此時 $k \geqslant \frac{3}{4}2^\gamma$, 故當 $s \geqslant 3k > 2^\gamma$ 時, (1) 式即有解.

2_2) $p>2$, $p-1|k$. 此時 $k\geqslant p^\gamma(p-1)>\frac{1}{3}p^\gamma$, 故當 $s\geqslant 3k>p^\gamma$ 時, (1) 式顯然有解.

2_3) $p>2$, $(p-1)\nmid k$, $p\nmid k$. 此時 $\gamma=1$. 由 $(p-1)\nmid k$ 及定理 3.7.2 及 3.7.3, 可知當 x 過縮系, mod p, x^k 給與

$$d=\frac{p-1}{(k,p-1)}>1$$

個互不同餘的數, mod p. 由定理 1, $x_1^k+\cdots+x_s^k$ $(p\nmid x_1,\cdots,x_s)$ 給與

$$\min\left(d+(d-1)(s-1),p\right)$$

個互不同餘的數, mod p. 當

$$s\geqslant 2k>\frac{p-1}{\frac{1}{2}d}\geqslant\frac{p-1}{d-1}$$

時,

$$\min\left(d+(d-1)(s-1),p\right)=p.$$

故定理成立.

2_4) $p>2$, $(p-1)\nmid k$, $k=p^\gamma k_0$, $p\nmid k_0$. 由於

$$x^{p^\gamma k_0}\equiv x^{k_0}\pmod p$$

及 $(p-1)\nmid k_0$, 所以 x^k 至少經過 $(p-1)/(p-1,k_0)$ (>1) 個互不同餘的數, mod p, 故

$$x_1^k+\cdots+x_s^k,\quad p\nmid x_1\cdots x_s$$

給與

$$\min\left(\frac{p-1}{(p-1,k_0)}+\left(\frac{p-1}{(p-1,k_0)}-1\right)(s-1),\ p^\gamma\right)$$

個互不同餘的數, mod p^γ. 由

$$s-1\geqslant 3k\geqslant\frac{2pk}{p-1}\geqslant\frac{p^\gamma}{\frac{1}{2}\frac{p-1}{(k_0,p-1)}}\geqslant\frac{p^\gamma-1}{\frac{p-1}{(k_0,p-1)}-1},$$

可知 $x_1^k+\cdots+x_s^k$ $(p\nmid x_1\cdots x_s)$ 給與 p^γ 個互不同餘的數. 定理卽完全證明.

§4. 初等方法示例.

關於 Waring 問題之研究, 初等方法一般並不能得出較好之結果. 現在介紹數例. 對特殊之 k 證明 $G(k)$ 或 $g(k)$ 有上限存在. 有時也能求出上限, 但該上限是不甚精密者.

定理 1. $g(4) \leqslant 50$.

證: 今由恆等式

$$6(a^2+b^2+c^2+d^2)^2 = (a+b)^4+(a-b)^4+(c+d)^4+(c-d)^4+ \\ +(a+c)^4+(a-c)^4+(b+d)^4+(b-d)^4+ \\ +(a+d)^4+(a-d)^4+(b+c)^4+(b-c)^4 \qquad (1)$$

出發. 由於 $a^2+b^2+c^2+d^2$ 可表任意一整數,故左邊實際上表 $6x^2$ 而 x 是任一整數。

任一整數 n 可以表爲

$$n = 6N + r, \qquad r = 0, 1, 2, 3, 4, 5.$$

故

$$n = 6(x_1^2+x_2^2+x_3^2+x_4^2)+r.$$

再經恆等式 (1) $6x_1^2$ 可以表爲 12 個四次方之和. 故 n 乃 $4 \times 12 + 5 = 53$ 個四次方數之和.

再進一步,若 $n \geqslant 81$, 則可以表爲

$$n = 6N + t,$$

此處 $N \geqslant 0$ 及 $t = 0, 1, 2, 81, 16$ 及 17, 此五數 $\equiv 0, 1, 2, 3, 4, 5 \pmod 6$. 而

$$1 = 1^4,\ 2 = 1^4+1^4,\ 81 = 3^4,\ 16 = 2^4,\ 17 = 2^4+1.$$

故同上法,若 $n \geqslant 81$, 則可以表爲 $4 \times 12 + 2 = 50$ 個四次方數之和.

當 $n \leqslant 80$ 時,易於算出: 若 $n \leqslant 50$, 顯然有 $n = n \cdot 1^4$, 若 $50 < n \leqslant 80$, 則 $n = 3 \cdot 2^4 + (n-48) \cdot 1^4$, 此爲 $3 + n - 48 < 50$ 個四方數之和.

同法由恆等式

$$5040(a^2+b^2+c^2+d^2)^4 = \\ = 6\sum(2a)^8+60\sum(a \pm b)^8+\sum(2a \pm b \pm c)^8+6\sum(a \pm b \pm c \pm d)^8, \qquad (2)$$

可以證明 $g(8) < \infty$. 此式右邊共有 840 個 8 次方. 又因 $n \leqslant 5039$ 都可表成 $\leqslant 273$ 個 1 及 2 的 8 次方之和,故由此可得

$$g(8) \leqslant 840g(4) + 273 \leqslant 42273.$$

定理 2. $G(3) \leqslant 13$.

證: 今由等式

$$\sum_{i=1}^{4}((z^3+x_i)^3+(z^3-x_i)^3)=8z^9+6z^3(x_1^2+x_2^2+x_3^2+x_4^2) \tag{1}$$

開始. 若一數可以表成

$$8z^9+6mz^3, \quad 0\leqslant m\leqslant z^6, \tag{2}$$

則由 (1) 此數一定可以表爲 8 個立方數之和. 因爲 m 可以表爲 $x_1^2+x_2^2+$ $+x_3^2+x_4^2$, 且 $x_i\leqslant z^3$.

命 z 爲 6 除餘 1 之正整數. I_z 代表隔間

$$\phi(z)=11z^9+(z^3+1)^3+125z^3\leqslant n\leqslant 14z^9=\psi(z). \tag{3}$$

顯然當 z 充分大時有

$$\phi(z+6)<\psi(z), \tag{4}$$

卽 I_z 皆爲互相銜接之隔間. 卽當 n 充分大時,必有一 z 使 (3) 式成立.

由下式定義 r, s 及 N:

$$n\equiv 6r \pmod{z^3}, \quad 1\leqslant r\leqslant z^3,$$
$$n\equiv s+4 \pmod 6, \quad 0\leqslant s\leqslant 5,$$
$$N=(r+1)^3+(r-1)^3+2(z^3-r)^3+(sz)^3.$$

如此則

$$0<N<(z^3+1)^3+3z^9+125z^3=\phi(z)-8z^9\leqslant n-8z^9,$$

故

$$8z^9<n-N<14z^9. \tag{5}$$

今往證明 $n-N$ 可以表爲 (2) 之形式.

$$n-N\equiv 6r-(r+1)^3-(r-1)^3+2r^3\equiv 0\equiv 8z^9 \pmod{z^3},$$

又

$$n-N\equiv s+4-(r+1)-(r-1)-2(z^3-r)-sz\equiv$$
$$\equiv s+4-z(s+2)\equiv 2\equiv 8\equiv 8z^9 \pmod 6,$$

故 $n-N-8z^9$ 爲 $6z^3$ 之倍數,卽

$$n=N+8z^9+6mz^3.$$

若能證明 $0\leqslant m\leqslant z^6$, 則定理已明. 但此點由 (5) 立刻推得.

定理 3. $g(3)\leqslant 13$.

證: 1) 先算出若 $z\geqslant 373$, 則 $\phi(z+6)\leqslant\psi(z)$,或,當 $t\geqslant 379$ 時

$$11t^9+(t^3+1)^3+125t^3\leqslant 14(t-6)^9,$$

即

$$14\left(1-\frac{6}{t}\right)^9\geqslant 12+\frac{3}{t^3}+\frac{128}{t^6}+\frac{1}{t^9}. \tag{6}$$

由於當 $0<\delta<1$ 時 $(1-\delta)^m\geqslant 1-m\,\delta$, 故

$$\left(1-\frac{6}{t}\right)^9\geqslant 1-\frac{54}{t}.$$

故若能證明

$$14\left(1-\frac{54}{t}\right)\geqslant 12+\frac{3}{t^3}+\frac{128}{t^6}+\frac{1}{t^9},$$

或若能證明

$$2(t-7\times 54)\geqslant \frac{3}{t^2}+\frac{128}{t^5}+\frac{1}{t^8},$$

則 (6) 式成立. 由於 $t>7\times 54+1=379$, 故 (6) 式成立.

即當 $z=373$ 以上, 諸 I_z 是衔接的. 即當

$$n\geqslant 14\,(373)^9$$

時必落在一個 I_z 中. 又 $10^{25}>14\,(373)^9$. 故任一整數 $\geqslant 10^{25}$ 者必可表爲十三個立方數之和.

2) 再證不大於 10^{25} 之數也是十三個立方數之和. 先造表可知小於 40000 之數除去 23 及 239 外皆是 8 個立方數之和, 而 23 及 239 是九個立方數之和. 即若 $240\leqslant n\leqslant 40000$ 則 n 是八個立方數之和. 又若 $N\geqslant 1$ 及 $m=$ $=[N^{1/3}]$, 則

$$N-m^3=(N^{1/3})^3-m^3\leqslant 3N^{2/3}(N^{1/3}-m)<3N^{2/3}.$$

假定

$$240\leqslant n\leqslant 10^{25},$$

並命

$$n=240+N,\quad 0\leqslant N<10^{25},$$

則

$$N=m^3+N_1,\qquad m=[N^{1/3}],\qquad 0<N_1<3N^{2/3},$$

$$N_1=m_1^3+N_2,\qquad m_1=[N_1^{1/3}],\qquad 0<N_2<3N_1^{2/3},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$N_4=m_4^3+N_5,\qquad m_4=[N_4^{1/3}],\qquad 0<N_5<3N_4^{2/3}.$$

故

$$n = 240 + N = 240 + N_5 + m^3 + m_1^3 + m_2^3 + m_3^3 + m_4^3.$$

由於

$$0 < N_5 \leqslant 3N_4^{2/3} \leqslant 3(3N_3^{2/3})^{2/3} \leqslant \cdots \leqslant$$

$$\leqslant 3 \cdot 3^{2/3} \cdot 3^{(2/3)^2} 3^{(2/3)^3} 3^{(2/3)^4} N^{(2/3)^5} =$$

$$= 27\left(\frac{N}{27}\right)^{(2/3)^5} < 27\left(\frac{10^{25}}{27}\right)^{(2/3)^5} < 35000.$$

故

$$240 \leqslant 240 + N_5 < 35240 < 40000,$$

卽 $240 + N_5$ 可以表爲八個立方數之和，故得定理.

由恆等式

$$60(a^2 + b^2 + c^2 + d^2)^3 = \sum (a \pm b \pm c)^6 + 2\sum (a \pm b)^6 + 36\sum a^6,$$

可以證明 $g(6) \leqslant 184g(3) + 59 \leqslant 2451$.

§ 5. 有正負號之較易問題.

命 $v(k)$ 爲最小之自然數 s，使任一整數

$$n = \pm x_1^k \pm x_2^k \pm \cdots \pm x_s^k$$

有解. 卽可以取 $\pm$ 號並整數 x 使上式成立. 顯然

$$v(k) \leqslant g(k).$$

對此問題，$v(k)$ 的存在是十分顯然的.

定理 1. $v(k) \leqslant 2^{k-1} + \frac{1}{2}k!$.

證此定理須用次之定理.

定理 2. 命 $\Delta f(x) = f(x+1) - f(x)$，$\Delta^{m+1}f(x) = \Delta(\Delta^m f(x))$. 則得

$$\Delta^{k-1} x^k = k!\, x + d,$$

此 d 是一整數.

若 $f(x)$ 是一 k 次多項式其首項係數爲 a 者，則 $\Delta f(x)$ 是一 $(k-1)$ 次多項式其首項係數爲 ka. 續行此法可得定理 2.

定理 1 之證明: $\Delta^{k-1} x^k$ 可以看成是 2^{k-1} 個 $\pm x^k$ 之和.

任與一整數 n 可以表成爲

$$n-d=k!\,x+l, \qquad |l|\leqslant\frac{1}{2}k!$$

之形式,卽

$$n=\Delta^{k-1}x^k+l.$$

由於 $2^{k-1}+l\leqslant 2^{k-1}+\frac{1}{2}k!$. 故得定理.

定理 3. $v(k)\leqslant G(k)+1$.

證: 取 y 充分大使 $n+y^k$ 大於某一充分大之數. 由 $G(k)$ 之定義, 故 $n+y^k=x_1^k+\cdots+x_{G(k)}^k$. 故得定理.

定理 4. $v(2)=3$.

證: 由定理 1 已知 $v(2)\leqslant 3$. 但 6 不能表爲二平方數,因 6 不是二平方數之和,而二平方數之差 x^2-y^2 或爲奇數, 或爲 4 之倍數. 故 $v(2)>2$.

定理 5. $v(3)$ 爲 4 或 5 (未解決其爲 4 抑 5, 推測是 4).

證: 由

$$n^3-n\equiv 0 \pmod 6,$$

可命 $n^3-n=6x$. 故

$$n=n^3-(x+1)^3-(x-1)^3+2x^3.$$

故 $v(3)\leqslant 5$.

又

$$y^3\equiv 0, 1 \text{ 或 } -1 \pmod 9,$$

故若 $n=9m\pm 4$ 必不可能表爲三立方數之和. 故 $v(3)\geqslant 4$.

關於此問題柯召曾驗證絕對值 $\leqslant 100$ 之整數皆可表成四個立方數之和.

定理 6. $v(4)$ 爲 9 或 10.

證: 由

$$48x+4=2(2x+3)^4+(2x+6)^4+2(2x^2+8x+11)^4-(2x^2+8x+10)^4-\\-(2x^2+8x+12)^4;$$

$$48x-14=2(2x+5)^4+(2x+8)^4+(x^2+6x+9)^4+(x^2+6x+12)^4-\\-(x^2+6x+8)^4-(x^2+6x+13)^4;$$

$$24x=(4y+11)^4+(2y-87)^4+(y-9)^4+(y-41)^4+(y-83)^4+(y+125)^4+\\+(y^2+603)^4+(y^2+625)^4-(y^2+602)^4-(y^2+626)^4,$$

式中 $y=x-10319691$;

$$24x-8=(4y+11)^4+(2y-87)^4+(y+883)^4+(y-933)^4+(y-975)^4+$$
$$+(y+1017)^4+(y^2+39851)^4+(y^2+39873)^4-(y^2+39850)^4-$$
$$-(y^2+39874)^4,$$

式中 $y=x-120858614086$.

於上之四式中將 x 變爲 $-x$, 則同樣可得關於 $48x-4$, $48x+14$, $24x+8$ 的表示式. 由是容易看出,若 n 爲 8 之倍數,則 n 可表爲 10 個 4 次方之和. 若 n 非 8 之倍數,則 n 可寫成

$$n=48z+\gamma, \qquad -24<\gamma<24,$$

吾人容易證明常有整數, x_1, x_2, x_3 使

$$\gamma \pm x_1^4 \pm x_2^4 \pm x_3^4 \equiv \pm 4, \pm 14 \pmod{48}.$$

由是卽得 $v(4) \leqslant 10$.

因 $\pm y^4 \equiv 0, \pm 1 \pmod{16}$, 故形如 $16x+8$. 之數至少需要 8 個 4 次方來表示, 且每項皆同號才可. 但 24, 104 等數卽不能表示成如是之形狀,故 $v(4) \geqslant 9$. 定理卽已完全證明.

§ 6. 等冪和問題.

命 $N(k)$ 是最小的整數 s, 有 $x_1, \cdots, x_s$; $y_1, \cdots, y_s$ 存在,但 $y_1, \cdots, y_s$ 並非由 $x, \cdots, x_s$ 顚倒次序而得者,使

$$\left.\begin{array}{l} x_1+\cdots+x_s=y_1+\cdots+y_s, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x_1^k+\cdots+x_s^k=y_1^k+\cdots+y_s^k. \end{array}\right\} \tag{1}$$

又以 $M(k)$ 表最小之整數 s, 使上解並適合

$$x_1^{k+1}+\cdots+x_s^{k+1} \neq y_1^{k+1}+\cdots+y_s^{k+1}. \tag{2}$$

定理 1. $M(k) \geqslant N(k) \geqslant k+1$.

證: 由

$$\begin{array}{l} x_1+\cdots+x_k=y_1+\cdots+y_k, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x_1^k+\cdots+x_k^k=y_1^k+\cdots+y_k^k, \end{array}$$

可知 $(x-x_1)\cdots(x-x_k)=(x-y_1)\cdots(x-y_k)$, 故 $x_1, \cdots, x_k$ 是由 $y_1, \cdots, y_k$

變換次序而得者.

定理 2. $N(k) \leqslant M(k) \leqslant 2^k$.

證: 若 $x_1, \cdots, x_s; y_1, \cdots, y_s$ 是 (1) 及 (2) 之解,則

$$\sum_{i=1}^{s}((x_i+d)^h+y_i^h)=\sum_{i=1}^{s}(x_i^h+(y_i+d)^h),\quad 1\leqslant h\leqslant k+1,\tag{3}$$

$$\sum_{i=1}^{s}((x_i+d)^{k+2}+y_i^{k+2})\neq\sum_{i=1}^{s}(x_i^{k+2}+(y_i+d)^{k+2}).\tag{4}$$

此二式之證明,可展開 (3),(4) 並用 (1),(2) 卽得.

由是,若 $M(k)$ 存在,則取 $s=M(k)$, 立得

$$M(k+1)\leqslant 2M(k).$$

但 $M(1)=N(1)=2$, 故由歸納法卽得定理.

定理 3. $N(k)\leqslant\frac{1}{2}k(k+1)+1$.

證: 設 $n>s!\,s^k$. 令 $a_i\ (i=1,2,\cdots,s)$ 跑過 $1,2,\cdots,n$. 則得 n^s 組 $a_1,a_2,\cdots,a_s$. 固定 $a_1,a_2,\cdots,a_s$, 將其任意加以排列, 則至多得 $s!$ 組. 故此 n^s 組 $a_1,a_2,\cdots,a_s$ 中,至少有 $\frac{n^s}{s!}$ 組,其中無一組是他一組的某一排列.

記

$$s_h(a)=a_1^h+a_2^h+\cdots+a_s^h,\quad h=1,2,\cdots,k.$$

則

$$s\leqslant s_h(a)\leqslant sn^h.$$

故至多有

$$\prod_{h=1}^{k}(sn^h-s+1)<s^k\,n^{\frac{1}{2}k(k+1)}$$

組不同的

$$s_1(a),\ s_2(a),\cdots,s_k(a).\tag{5}$$

取 $s=\frac{1}{2}k(k+1)+1$, 則由 $n>s!s^k$, 卽得

$$s^k\,n^{\frac{1}{2}k(k+1)}=s^k\,n^{s-1}<\frac{n^s}{s!}.$$

故至少有兩組不相同的 $a_1,a_2,\cdots,a_s$ 使 (5) 取同樣數值. 因此兩組中一組非他一組之某一排列. 故 $N(k)\leqslant s$, 卽得定理.

今以

$$[a_1,\cdots,a_s]_k=[b_1,\cdots,b_s]_k$$

表示 (1) 及 (2).

由定理 1 及以下諸例,卽得

定理 4. 若 $k \leqslant 9$, 則 $M(k)=N(k)=k+1$.

$$[0, 3]_1=[1, 2]_1,$$

$$[1, 2, 6]_2=[0, 4, 5]_2,$$

$$[0, 4, 7, 11]_3=[1, 2, 9, 10]_3,$$

$$[1, 2, 10, 14, 18]_4=[0, 4, 8, 16, 17]_4,$$

$$[0, 4, 9, 17, 22, 26]_5=[1, 2, 12, 14, 24, 25]_5,$$

$$[0, 18, 27, 58, 64, 89, 101]_6=[1, 13, 38, 44, 75, 84, 102]_6,$$

$$[0, 4, 9, 23, 27, 41, 46, 50]_7=[1, 2, 11, 20, 30, 39, 48, 49]_7,$$

$$[0, 24, 30, 83, 86, 133, 157, 181, 197]_8=[1, 17, 41, 65, 112, 115, 168, 174, 198]_8,$$

$$[0, 3083, 3301, 11893, 23314, 24186, 35607, 44199, 44417, 47500]_9=$$

$$=[12, 2865, 3519, 11869, 23738, 23762, 35631, 43981, 44635, 47488]_9.$$

§7. Prouhet-Tarry 問題.

本節及下節之目的,是在證明

$$M(k) \leqslant (k+1)\left(\left[\frac{\log \frac{1}{2}(k+2)}{\log\left(1+\frac{1}{k}\right)}\right]+1\right) \sim k^2 \log k .$$

實際上,我們所得出的結果比此爲多.

在證明此不等式之前,我們先證明幾條引理. 本節及下節中之常數 $c_1, c_2, \cdots$ 及符號 O 中所含之常數皆僅與 k 有關. 且 $c_1, c_2, \cdots$ 皆爲正數.

定理 1 (Буняковский-Schwarz). 若 a_i, b_i $(i=1, 2, \cdots, n)$ 爲實數, 則

$$\left(\sum_{i=1}^{n} a_i b_i\right)^2 \leqslant\left(\sum_{i=1}^{n} a_i^2\right)\left(\sum_{i=1}^{n} b_i^2\right),$$

等號僅當 $\frac{a_1}{b_1}=\frac{a_2}{b_2}=\cdots=\frac{a_n}{b_n}$ 時成立.

證: 此可由

$$\sum a_i^2 \sum b_i^2-\left(\sum a_i b_i\right)^2=\sum_{i<j}\left(a_i b_j-b_i a_j\right)^2 \geqslant 0$$

立刻得出.

定理 2. 任與一數 H, 必存在一組僅與 k 及 H 有關之正整數 $a_1, \cdots, a_k$, 使行列式

$$D_k = \begin{vmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_k \\ \cdots & \cdots & \cdots \\ a_1^{k-1} & \cdots & a_k^{k-1} \end{vmatrix}$$

之主對角線上諸元素之積大於 H 乘 D_k 之展開式中其餘各項之絕對值之和.

證: 我們用歸納法來證明本定理. 設 $j \leqslant k$, 以 $\varphi_j(a_1, \cdots, a_j)$ 表示 D_j 之主對角線上諸元素之積減去 H 乘 D_j 之展開式中其餘各項之絕對值之和, 則顯然有

$$\varphi_j(a_1, \cdots, a_j) = a_j^{j-1}\varphi_{j-1}(a_1, \cdots, a_{j-1}) - H\psi(a_1, \cdots, a_j),$$

式中 ψ 爲 a_j 之 $j-2$ 次多項式. 由假定, 我們可取 $a_1, \cdots, a_{j-1}$ 使 $\varphi_{j-1}(a_1, \cdots, a_{j-1}) > 0$. 對此組 $a_1, \cdots, a_{j-1}$, 我們顯然可取 a_j 使 $\varphi_j > 0$. 但 $\varphi_1(a_1) = 1$, 故得定理.

定理 3. 設 $a_1, \cdots, a_k$ 爲滿足定理 2 之一組正整數. 又設 $Q \geqslant 1$, $X_1, \cdots, X_k$ 爲分別屬於區間

$$a_i Q \leqslant X_i \leqslant 2a_i Q \qquad (i = 1, 2, \cdots, k)$$

之正整數. 設 N 爲如是之 $(X_1, \cdots, X_k)$ 中, 使

$$X_1^k + \cdots + X_k^k,\ X_1^{k-1} + \cdots + X_k^{k-1}, \cdots, X_1 + \cdots + X_k$$

分別落入長爲

$$O(Q^{k-1}),\ O(Q^{k-2}), \cdots, O(Q),\ O(1)$$

之已與區間者之組數. 則

$$N = O(1).$$

證: 若 $(X_1, \cdots, X_k)$ 與 $(X_1', \cdots, X_k')$ 爲滿足定理中諸條件之二組. 則顯然有

$$X_1^k - X_1'^k + \cdots + X_k^k - X_k'^k = O(Q^{k-1}),$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$X_1 - X_1' + \cdots + X_k - X_k' = O(1).$$

令 $Y_i = X_i - X'_i$. 則得

$$A_{11} Y_1 + \cdots + A_{1k} Y_k = O(Q^{k-1}),$$
$$\cdots\cdots\cdots\cdots$$
$$A_{k1} Y_1 + \cdots + A_{kk} Y_k = O(1).$$

於此

$$A_{ij} = X_j^{k-i} + X_j^{k-i-1} X'_j + \cdots + X'^{k-i}_j, \quad (1 \leqslant i, j \leqslant k).$$

顯而易見,

$$(k-i+1)(a_j Q)^{k-i} \leqslant A_{ij} \leqslant (k-i+1)(2a_j Q)^{k-i}.$$

行列式 $|A_{k-i+1,j}|$ 之主對角線上諸元素之積與上定理中之 D_k 之對應項之商顯然大於

$$k!\, Q^{k-1+k-2+\cdots+2+1} = k!\, Q^{\frac{1}{2}k(k-1)}.$$

而 $|A_{k-i+1,j}|$ 之展開式中其餘各項之絕對值與 D_k 中對應項之絕對值之商顯然小於

$$2^{\frac{1}{2}k(k-1)}\, k!\, Q^{\frac{1}{2}k(k-1)}.$$

由定理 2, 取 $H = 2^{\frac{1}{2}k(k-1)}$, 即得

$$\left| \, |A_{ij}| \, \right| \geqslant c_1 Q^{\frac{1}{2}k(k-1)}.$$

容易看出

$$\begin{vmatrix} O(Q^{k-1}) & A_{12} \cdots A_{1k} \\ \cdots\cdots & \cdots\cdots\cdots\cdots \\ O(1) & A_{k2} \cdots A_{kk} \end{vmatrix} = O(Q^{\frac{1}{2}k(k-1)}).$$

由是卽得

$$Y_1 = O(1).$$

同法可得

$$Y_2 = O(1), \cdots, Y_k = O(1).$$

由是定理卽已證明.

定理 4. 如定理 3 之假定. 設 $\lambda_1 \geqslant 0, \lambda_2 \geqslant 0, \cdots, \lambda_k \geqslant 0$. 則 $(X_1, \cdots, X_k)$ 中使

$$X_1^k + \cdots + X_k^k, \quad X_1^{k-1} + \cdots + X_k^{k-1}, \cdots, X_1 + \cdots + X_k$$

分別落入長爲

$$O(Q^{k+\lambda_k - 1}), \quad O(Q^{k+\lambda_{k-1} - 2}), \cdots, \quad O(Q^{\lambda_1})$$

之已與區間者之組數至多爲

$$O(Q^{\lambda_1+\cdots+\lambda_k}).$$

證: 因長爲 $O(Q^{k-i+\lambda_{k-i+1}})$ 之區間可以分爲 $O(Q^{\lambda_{k-i+1}})$ 個長爲 $O(Q^{k-i})$ 之區間. 由定理 3, 立得本定理.

今設 $\beta=\frac{k}{k+1}$, $a_1, \cdots, a_{k+1}$ 爲滿足定理 2 中所說條件之一組正整數 (於該定理中以 $k+1$ 代 k). 又設

$$a_u Q^{\beta^{v-1}} \leqslant y_{uv} \leqslant 2a_u Q^{\beta^{v-1}} \quad (1\leqslant u\leqslant k+1,\ 1\leqslant v\leqslant l).$$

以 $r(n_1, \cdots, n_k)$ 記方程組

$$\sum_{u=1}^{k+1}\sum_{v=1}^{l} y_{uv}^h = n_h \quad (1\leqslant h\leqslant k)$$

之解數. 我們現來證明下列定理:

定理 5. 存在一組整數 $N_1, \cdots, N_k$, 使

$$r(N_1, \cdots, N_k) \geqslant c_1 Q^{(k+1)^2(1-\beta^l)-\frac{1}{2}k(k+1)}.$$

證: 諸 (y_{uv}) 的不同的組數顯然

$$\geqslant \frac{1}{2}\prod_{u=1}^{k+1}\prod_{v=1}^{l} a_u Q^{\beta^{v-1}} \geqslant c_2 Q^{(k+1)(1+\beta+\cdots+\beta^{l-1})} =$$
$$= c_2 Q^{(k+1)^2(1-\beta^l)}.$$

因 $|n_h|\leqslant c_3 Q^h$, 故諸 (n_h) 的不同的組數

$$\leqslant c_4 Q^{1+2+\cdots+k} = c_4 Q^{\frac{1}{2}k(k+1)}.$$

故必存在一組整數 $N_1, \cdots, N_k$, 使

$$r(N_1, \cdots, N_k) \geqslant \frac{c_2}{c_4} Q^{(k+1)^2(1-\beta^l)-\frac{1}{2}k(k+1)}.$$

定理 6. 方程組

$$\sum_{u=1}^{k+1}\sum_{v=1}^{l} y_{uv}^h = N_h \quad (1\leqslant h\leqslant k+1)$$

的解的數目 $\leqslant c_5 Q^{\frac{1}{2}k(k+1)(1-\beta^l)}$.

證: 由

$$\sum_{u=1}^{k+1} y_{u1}^h = N_h - \sum_{u=1}^{k+1}\sum_{v=2}^{l} y_{uv}^h \quad (1\leqslant h\leqslant k+1)$$

及

$$a_u Q^{\beta^{v-1}} \leqslant y_{uv} \leqslant 2a_u Q^{\beta^{v-1}} \quad (1\leqslant u\leqslant k+1,\ 1\leqslant v\leqslant l)$$

可知

$$y_{11}^{k+1}+\cdots+y_{k+1,1}^{k+1},\ y_{11}^{k}+\cdots+y_{k+1,1}^{k},\cdots,\ y_{11}+\cdots+y_{k+1,1}$$

分別落入長為

$$O(Q^{(k+1)\beta}),\quad O(Q^{k\beta}),\cdots,\quad O(Q^{\beta})$$

之一區間內. 於定理 4 中取 $\lambda_u=u\,\beta-(u-1)\geqslant 0$, 則由

$$\sum_{u=1}^{k+1}\{u\beta-(u-1)\}=\frac{1}{2}\beta(k+1)(k+2)-\frac{1}{2}k(k+1)=\frac{1}{2}k,$$

卽知 $(y_{11},\cdots,y_{k+1,1})$ 的組數為 $O(Q^{\frac{1}{2}k})$.

對於固定的 $y_{11},\cdots,y_{k+1,1}$, 和數

$$y_{12}^{k+1}+\cdots+y_{k+1,2}^{k+1},\cdots,\ y_{12}+\cdots+y_{k+1,2}$$

顯然分別落入長為

$$O(Q^{(k+1)\beta^2}),\quad O(Q^{k\beta^2}),\cdots,\quad O(Q^{\beta^2})$$

之一區間內. 於定理 4 中以 Q^{β} 代 Q, 卽知 $y_{12},\cdots,y_{k+1,2}$ 的不同組數為 $O(Q^{\frac{1}{2}k\beta})$. 如是繼續進行,卽得定理.

§8. 續

定理 1. 設 $W(k,s)$ 為使方程組

$$\sum_{i=1}^{s}x_{i1}^{h}=\sum_{i=1}^{s}x_{i2}^{h}=\cdots=\sum_{i=1}^{s}x_{ij}^{h}\quad(1\leqslant h\leqslant k),$$

$$\sum_{i=1}^{s}x_{ip}^{k+1}\neq\sum_{i=1}^{s}x_{iq}^{k+1},\quad(p\neq q,\ 1\leqslant p,q\leqslant j)$$

有整數解之最小整數 s, 則

$$W(k,j)\leqslant(k+1)\left(\left[\frac{\log\frac{1}{2}(k+2)}{\log\left(1+\frac{1}{k}\right)}\right]+1\right).$$

證: 此定理顯然為下定理之一直接推論:

定理 2. 設

$$s\geqslant(k+1)\left(\left[\frac{\log\frac{1}{2}(k+2)}{\log\left(1+\frac{1}{k}\right)}\right]+1\right).$$

則對任與之 j 必存在整數

$$N_1, \cdots, N_k;\quad M_1, \cdots, M_j\qquad (M_{t_1} \neq M_{t_2},\ \text{若}\ t_1 \neq t_2)$$

使方程組

$$R_t(1 \leqslant t \leqslant j): \begin{cases} \sum_{i=1}^{s} x_{it}^h = N_h & (1 \leqslant h \leqslant k), \\ \sum_{i=1}^{s} x_{it}^{k+1} = M_t & (x_{it} \geqslant 0) \end{cases}$$

有解。

證： 設 $r(N_1, \cdots, N_h)$ 如上節中所定義. 由定理 7.5, 有 $N_1, \cdots, N_h$, 使

$$r(N_1, \cdots, N_h) \geqslant c_1\, Q^{(k+1)^2(1-\beta^l)-\frac{1}{2}k(k+1)}.$$

對方程組

$$\sum_{u=1}^{k+1} \sum_{v=1}^{l} y_{uv}^h = N_h \qquad (1 \leqslant h \leqslant k)$$

之一組解 (y_{uv}), 顯然有一數 M, 使

$$\sum_{u=1}^{k+1} \sum_{v=1}^{l} y_{uv}^{k+1} = M.$$

若如是之 M 僅有 $e(\leqslant j-1)$ 個不同的值, 設為 $M_1, \cdots, M_e$, 則由定理 7.6, e 個方程組

$$\prod_i (1 \leqslant i \leqslant e): \begin{cases} \sum_{u=1}^{k+1} \sum_{v=1}^{l} y_{uv}^h = N_h & (1 \leqslant h \leqslant k), \\ \sum_{u=1}^{k+1} \sum_{v=1}^{l} y_{uv}^{k+1} = M_i \end{cases}$$

的解的數目 $\leqslant c_5 e Q^{\frac{1}{2}k(k+1)(1-\beta^l)}$. 由 M_i 之定義, 此 e 個方程組的解的數目應 $\geqslant r(N_1, \cdots, N_k)$. 另一方面, 若取 $l > \left\{\log\frac{1}{2}(k+2)/\log\left(1+\frac{1}{k}\right)\right\}$, 則當 Q 甚大時, 我們有

$$c_5 e Q^{\frac{1}{2}k(k+1)(1-\beta^l)} < c_1\, Q^{(k+1)^2(1-\beta^l)-\frac{1}{2}k(k+1)} \leqslant$$
$$\leqslant r(N_1, \cdots, N_k).$$

即得一矛盾, 吾人之定理即已證明。

第 十 九 章

Шнирельман 密 率

§1. 密率之定義及其歷史.

本章之目的在於證明以下之二重要定理:

"有一正整數 c 存在,凡正整數必可表爲不超過 c 個素數之和."

"命 k 表一正整數. 有一正整數 c_k (僅與 k 有關) 存在,凡正整數必可表爲不超過 c_k 個正整數之 k 方之和."

此二定理與 Гольдбах 及 Waring 問題之關係乃屬顯然. 並可說: 此二定理乃 Гольдбах 問題及 Waring 問題最基本但也最初步之結果. 此二定理各名爲 Гольдбах—Шнирельман 定理及 Waring-Hilbert 定理.

本章中將引進 Шнирельман 所創造之密率概念. 此概念極爲初等,但藉此概念彼證明了以上所述之歷史上著名定理, 本章關於 Гольдбах-Шнирельман 定理之證明稍異於 Шнирельман 之原證. 今將引用 Selberg 之方法以代替原來之 Brun 篩法.

在證明 Waring-Hilbert 定理時, 亦不用 Hilbert 原證及 Шнирельман 之證明. 而將根據 Линник 在 1943 年之證明,加以簡化及改變而得者.

在此二證明中 Шнирельман 之密率皆居重要地位,密率之定義如次:

定義 1. 命 $\mathfrak{A}$ 表一由一些互不相同的非負整數 a 所成之集合. 命 $A(n)$ 表 $\mathfrak{A}$ 中不大於 n 之正整數之個數, 即

$$A(n)=\sum_{1\leqslant a\leqslant n}1.$$

若有正數 α 存在,使對任一正整數 n 常有 $A(n)\geqslant \alpha n$, 則此集合稱爲有正密率之集合. 有此性質的最大的 α. 稱爲此集合之正密率.

顯然有次之簡單性質:

(i) 由於 $A(n)\leqslant n$, 故得 $\alpha\leqslant 1$.

(ii) 若 $\alpha=1$, 則 $A(n)=n$, 故 $\mathfrak{A}$ 中包有全部正整數.

習題. 命 τ 表一實數 $\geqslant 1$, 求出集合

$$1+[\tau(n-1)],\qquad n=1,2,\cdots$$

之密率.

§2. 和集及其密率.

今引入記號 $\mathfrak{B}$, b, $B(n)$, β 及 $\mathfrak{C}$, c, $C(n)$, γ, 其間之關係一如 $\mathfrak{A}$, a, $A(n)$, α 之間之關係,卽 $b\in\mathfrak{B}$, $B(n)=\sum\limits_{1\leqslant b\leqslant n}1$ 而 β 是 $\mathfrak{B}$ 集之正密率等.

定義: 所有的形如 $a+b$ $(a\in\mathfrak{A}, b\in\mathfrak{B})$ 之整數所成之集合稱爲 $\mathfrak{A}$, $\mathfrak{B}$ 之和集,以 $\mathfrak{C}$ 表之. 並表爲 $\mathfrak{A}+\mathfrak{B}=\mathfrak{C}$.

定理 1. 若 $\mathfrak{C}=\mathfrak{A}+\mathfrak{B}$, 及 $0\in\mathfrak{A}$, 則 $\gamma\geqslant\alpha+\beta-\alpha\beta$.

證: 由於 $\beta>0$, 故 1 在 $\mathfrak{B}$ 中. 則下面三類數均爲 $\mathfrak{C}$ 中之正整數,不大於 n 且互不相同.

(i) 將 $\mathfrak{B}$ 中之 $b_1=1, b_2, \cdots, b_{B(n)}$ 依遞增之次序排列,因 $0\in\mathfrak{A}$, 故 $b_1, b_2, \cdots, b_{B(n)}$ 均在 $\mathfrak{C}$ 中,此種正整數共 $B(n)$ 個.

(ii) 對每一 v, $1\leqslant v\leqslant B(n)-1$, 當 $a\in\mathfrak{A}$ 且 $1\leqslant a\leqslant b_{v+1}-b_v-1$ 時,諸 $a+b_v$ 均爲正整數,在 $\mathfrak{C}$ 中,不大於 n 且互不相同. 蓋因

$$a+b_v\leqslant(b_{v+1}-b_v-1)+b_v=b_{v+1}-1\leqslant b_{B(n)}-1\leqslant n-1$$

且

$$a+b_v\geqslant 1+b_v,$$

故

$$1+b_v\leqslant a+b_v\leqslant b_{v+1}-1.$$

顯然,(i) 與 (ii) 中之諸正整數互不相同. 對每一 v, $1\leqslant v\leqslant B(n)-1$, 共有 $A(b_{v+1}-b_v-1)$ 個 $a+b_v$.

(iii) 當 $a\in\mathfrak{A}$, $1\leqslant a\leqslant n-b_{B(n)}$ 時,諸 $a+b_{B(n)}$ 均爲正整數,在 $\mathfrak{C}$ 中,不大於 n 且互不相同. 因 $a+b_{B(n)}\geqslant 1+b_{B(n)}$, 故 (iii) 中之諸正整數亦與 (i), (ii) 中者不同,且諸 $a+b_{B(n)}$ 共有 $A(n-b_{B(n)})$ 個.

由 (i), (ii), (iii) 之結果,可知

$$C(n)\geqslant B(n)+\sum_{v=1}^{B(n)-1}A(b_{v+1}-b_v-1)+A(n-b_{B(n)})\geqslant$$

$$\geqslant B(n) + \sum_{\nu=1}^{B(n)-1} \alpha(b_{\nu+1} - b_\nu - 1) + \alpha(n - b_{B(n)}) =$$
$$= B(n) + \alpha\{b_{B(n)} - b_1 - (B(n) - 1) + n - b_{B(n)}\} =$$
$$= B(n) + \alpha\{n - B(n)\} \geqslant (1-\alpha)\beta n + \alpha n =$$
$$= n(\alpha + \beta - \alpha\beta),$$

因此，$\frac{C(n)}{n} \geqslant \alpha + \beta - \alpha\beta$，$\gamma \geqslant \alpha + \beta - \alpha\beta$.

附記：此並非和集密率之最佳定理．而最佳之結果應爲 $\gamma \geqslant \min(1, \alpha+\beta)$．此結果在 1942 年爲 Mann 所證明．其證明甚爲複雜，並對本章之主要結果無基本上之改進，故不列入本書之範圍．今取 $\mathfrak{A}$ 及 $\mathfrak{B}$ 皆爲與 1 同餘之正整數，mod q．並假定 $\mathfrak{A}$ 還包有 0，則 $\mathfrak{A}+\mathfrak{B}$ 包有所有的與 1,2 同餘的正整數 mod q．顯然 $\mathfrak{A}$, $\mathfrak{B}$ 之密率爲 $\frac{1}{q}$ 及 $\mathfrak{A}+\mathfrak{B}$ 之密率爲 $\frac{2}{q}$．故 Mann 之結果爲最好．

定理 2. 若 $0 \in \mathfrak{A}$，$\alpha + \beta \geqslant 1$，則 $\mathfrak{C} = \mathfrak{A} + \mathfrak{B}$ 之密率 γ 爲 1，卽 $\mathfrak{C}$ 中包有所有的正整數．

證：假設 $\gamma \neq 1$，則 $\gamma < 1$，故有一最小的正整數 $n \notin \mathfrak{C}$．因 $\beta > 0$，故 $1 \in \mathfrak{B}$，又 $0 \in \mathfrak{A}$，故 $1 \in \mathfrak{C}$，而有 $n \geqslant 2$．又因 $0 \in \mathfrak{A}$ 故知 $n \notin \mathfrak{B}$.

考慮下面諸不大於 $n-1$ 的自然數 a 及 $n-b$：

$$a, \quad 1 \leqslant a \leqslant n-1, \quad a \in \mathfrak{A},$$
$$n-b, \quad 1 \leqslant b \leqslant n-1, \quad b \in \mathfrak{B}.$$

諸 a 與 $n-b$ 互不相同，否則必有 $a = n-b$，卽 $n = a+b \in \mathfrak{C}$，此爲一矛盾．又諸 a 與 $n-b$ 均不大於 $n-1$，故其個數不大於 $n-1$.

另一方面，諸 a 與 $n-b$ 之個數爲 $A(n-1)+B(n-1)$．因

$$A(n-1) \geqslant \alpha(n-1),$$
$$B(n-1) = B(n) \geqslant \beta n > \beta(n-1),$$

而有

$$A(n-1) + B(n-1) > \alpha(n-1) + \beta(n-1) = (\alpha+\beta)(n-1) \geqslant n-1.$$

此與諸 a 與 $n-b$ 之個數不大於 $n-1$ 矛盾．定理已明．

定理 3. 若 $\mathfrak{A}$ 包有 0，則任一正整數可以表爲 $\mathfrak{A}$ 中之

$$s_0 = 2\left[\frac{\log 2}{-\log(1-\alpha)}\right] + 2$$

個元素之和. 若 $\mathfrak{A}$ 不包有 0, 則任一正整數可以表爲 $\mathfrak{A}$ 中不多於 s_0 個元素之和.

證: 定理後半段可由前半段立卽得出,蓋因將元素 0 加於 $\mathfrak{A}$ 中形成新的集合 $\overline{\mathfrak{A}}$ 後,再利用定理前半段卽可. 今往證明定理之前半段.

$0 \in \mathfrak{A}$. 令 $\mathfrak{A}_h = \mathfrak{A} + \cdots + \mathfrak{A}$, 式中共 h 個 $\mathfrak{A}$ 相加. $\mathfrak{A}_h$ 之正密率以 α^h 表之. $\mathfrak{A}$ 之正密率爲 α, 則有 $\alpha_h \geqslant 1 - (1-\alpha)^h$. 今用歸納法,當 $h = 1$ 時,有 $\alpha_1 = \alpha$. 設當 $h - 1$ 時有

$$\alpha_{h-1} \geqslant 1 - (1-\alpha)^{h-1},$$

則因 $\mathfrak{A}_h = \mathfrak{A} + \mathfrak{A}_{h-1}$, 由定理 1,

$$\begin{aligned} \alpha_h &\geqslant \alpha + \alpha_{h-1} - \alpha\alpha_{h-1} = \alpha + (1-\alpha)\,\alpha_{h-1} \geqslant \\ &\geqslant \alpha + (1-\alpha)\{1 - (1-\alpha)^{h-1}\} = \\ &= 1 - (1-\alpha)^h. \end{aligned}$$

故當 $h = 1, 2, \cdots$ 時,恆有 $\alpha_h \geqslant 1 - (1-\alpha)^h$. 令

$$\frac{s_0}{2} = \left[\frac{\log 2}{-\log(1-\alpha)}\right] + 1 > \frac{\log 2}{-\log(1-\alpha)},$$

故有

$$(1-\alpha)^{s_0/2} \leqslant (1-\alpha)^{\frac{\log 2}{-\log(1-\alpha)}} = e^{-\frac{\log 2}{\log(1-\alpha)}\cdot\log(1-\alpha)} = \frac{1}{2}.$$

於是 $\alpha_{\frac{s_0}{2}} \geqslant 1 - (1-\alpha)^{s_0/2} \geqslant 1 - \frac{1}{2} = \frac{1}{2}$. 因 $0 \in \mathfrak{A}_{\frac{s_0}{2}}$ 由定理 2, 集合 $\mathfrak{A}_{s_0} = \mathfrak{A}_{\frac{s_0}{2}} + \mathfrak{A}_{\frac{s_0}{2}}$ 包有所有的正整數,故任一正整數可以表爲 $\mathfrak{A}$ 中之 s_0 個元素之和.

定理 4. 命 $\mathfrak{A}^*$ 表一非負整數之集合,其中允許重複. 命 $\mathfrak{A}$ 爲 $\mathfrak{A}^*$ 中不同元素所成之最大集合. 命 $r(a)$ 表示 a 在 $\mathfrak{A}^*$ 中出現之次數. 若對諸 $n \geqslant 1$ 常有

$$\frac{1}{n}\frac{\left(\sum\limits_{1\leqslant a\leqslant n} r(a)\right)^2}{\sum\limits_{1\leqslant a\leqslant n} r^2(a)} \geqslant \alpha'(>0),$$

則 $\mathfrak{A}$ 有正密率 $\alpha \geqslant \alpha'$.

證: 由 Буняковский-Schwarz 不等式 (定理 18.7.1) 可知

$$\left(\sum_{1\leqslant a\leqslant n} r(a)\right)^2 \leqslant \sum_{1\leqslant a\leqslant n} r^2(a) \sum_{1\leqslant a\leqslant n} 1^2 = A(n) \sum_{1\leqslant a\leqslant n} r^2(a),$$

故得

$$\frac{A(n)}{n} \geqslant \frac{1}{n}\Big(\sum_{1\leqslant a\leqslant n} r(a)\Big)^2 \Big/ \sum_{1\leqslant a\leqslant n} r^2(a) \geqslant \alpha' .$$

定理已明．

§ 3. **Гольдбах–Шнирельман 定理.**

在 §§3—5 中 $c, c_1, c_2, \cdots$ 皆表絕對正常數． §§3—5 之目的在於證明

定理 1. 有一正整數 c 存在，凡大於 1 之整數皆可表爲不超過 c 個素數之和．

定義 $\mathfrak{A}^*$ 爲 1 及所有的 p_1+p_2 之集合，此處 p_1, p_2 過所有的素數． 因之，$\mathfrak{A}^*$ 中可能有重複之元素． 再定義 $\mathfrak{A}$ 爲 $\mathfrak{A}^*$ 中不同元素之最大集合． 欲證定理 1 祇須證明

定理 2. $\mathfrak{A}$ 有正密率 c_1

由定理 2.3 可知任一正整數 m 可以表爲最多 s_0 個 $\mathfrak{A}$ 中之元素之和（卽若干個 1 及若干個形如 p_1+p_2 之整數之和）． 卽 m 是最多 $2s_0$ 個素數或 1 之和． 故對任一 $n>2$，可以有 $n=2+(n-2)=2+b\cdot 1+\Sigma p$，在此和號內素數 p 之個數 $\leqslant 2s_0-b$． 又易知 $2+b$ 可以表爲不超過 $b+1$ 個素數之和．因此，n 可以表爲不超過 $2s_0+1$ 個素數之和． 故得定理 1.

又命 $r(1)=1$ 及 $r(a)$ 爲 $\mathfrak{A}^*$ 中 a 出現之次數． 故

$$r(a)=\begin{cases} 1 \quad, & 若\ a=1, \\ \sum\limits_{p_1+p_2=a} 1, & 若\ a\geqslant 2. \end{cases}$$

定理 2.4 建議，今後之目的在於蕁求 $\sum\limits_{1\leqslant a\leqslant n} r(a)$ 之下限及 $\sum\limits_{1\leqslant a\leqslant n} r^2(a)$ 之上限， 前者不難獲得，後者將爲下節之主題．

定理 3. 若 $n\geqslant 2$，則

$$\sum_{1\leqslant a\leqslant n} r(a) \geqslant c_2 n^2/\log^2 n . \tag{1}$$

證： 設 $n\geqslant 4$． 由定理 5,6.2 得

$$\sum_{1\leqslant a\leqslant n} r(a) = 1 + \sum_{4\leqslant a\leqslant n}\ \sum_{p_1+p_2=a} 1 \geqslant$$

$$\geqslant \sum_{p_1, p_2 \leqslant n/2} 1 = \pi^2\left(\frac{1}{2}n\right) \geqslant$$

$$\geqslant \left(c_3 \frac{n}{2} \Big/ \log \frac{n}{2}\right)^2 \geqslant \frac{c_3^2}{4} \frac{n^2}{\log^2 n}.$$

若 $n = 2$ 或 3，易知 $\Sigma\, r(a) = 1$. 故祇須取 $c_2 = \min\left(\frac{c_3^2}{4}, \frac{\log^2 2}{4}, \frac{\log^2 3}{9}\right)$，卽得定理.

由定理 2.4 及 $r(1) = 1$，可知問題之焦點在於證明

定理 4. 若 $n \geqslant 2$，則

$$\sum_{1 \leqslant a \leqslant n} r^2(a) \leqslant c_4 \frac{n^3}{\log^4 n}. \tag{2}$$

換言之，若定理 4 已證明，則由

$$\frac{1}{n} \frac{\left(\sum_{1 \leqslant a \leqslant n} r(a)\right)^2}{\sum_{1 \leqslant a \leqslant n} r^2(a)} \geqslant \frac{1}{n} \frac{(c_2 n^2/\log^2 n)^2}{c_4 n^3/\log^4 n} = \frac{c_2^2}{c_4}$$

及定理 2.4 卽得出定理 2.

因此，今後僅須證明定理 4 卽足。

§ 4. Selberg 不等式.

本節中雖然可以不用，但是讀者不可不知以下之定理：

定理 1. 設 $a_i > 0$ $(i = 1, 2, \cdots, n)$ 及 b_i $(i = 1, 2, \cdots, n)$ 是固定的實數. 在條件 $\sum_{i=1}^{n} b_i x_i = 1$ 之下，$\sum_{i=1}^{n} a_i x_i^2$ 之極小值爲

$$\frac{1}{\sum_{i=1}^{n} \frac{b_i^2}{a_i}},$$

且當

$$x_i = \frac{\frac{b_i}{a_i}}{\sum_{i=1}^{n} \frac{b_i^2}{a_i}}$$

時取極值.

證: 由 Буняковский-Schwarz 不等式（定理 18.7.1）得知

$$\left(\sum_{i=1}^{n} a_i x_i^2\right)\left(\sum_{i=1}^{n} b_i^2 a_i^{-1}\right) \geqslant \left(\sum_{i=1}^{n} x_i b_i\right)^2 = 1.$$

故得

$$\sum_{i=1}^{n} a_i x_i^2 \geqslant \frac{1}{\sum_{i=1}^{n} b_i^2 a_i^{-1}}. \tag{1}$$

又由定理 18.7.1 知 (1) 式等號成立之充要條件爲有一實數 t_0 存在使

$$\sqrt{a_i}\, x_i = t_0 b_i \frac{1}{\sqrt{a_i}} \qquad (i = 1, 2, \cdots, n),$$

卽

$$x_i = b_i a_i^{-1} t_0 \qquad (i = 1, 2, \cdots, n).$$

故得

$$1 = \sum_{i=1}^{n} b_i x_i = \sum_{i=1}^{n} b_i^2 a_i^{-1} t_0,$$

卽

$$t_0 = \frac{1}{\sum_{i=1}^{n} b_i^2 a_i^{-1}}.$$

故得

$$x_i = \frac{b_i a_i^{-1}}{\sum_{i=1}^{n} b_i^2 a_i^{-1}} \qquad (i = 1, 2, \cdots, n). \tag{2}$$

定理已明.

定理 2 (A. Selberg). 設給一 M 個整數的集合 $\{b\}$, 能被正整數 k 所整除的 b 的個數是

$$\sum_{k|b} 1 = g(k) M + R(k), \tag{3}$$

此處 $R(k)$ 是餘項, 而 $g(k)$ 是正值的積性函數, 且 $g(p) < 1$.

令 N_ξ 表示 $\{b\}$ 中不能被 $\leqslant \xi$ 的素數所整除的 b 的個數, 則

$$N_\xi \leqslant \frac{M}{\sum_{1 \leqslant k \leqslant \xi} \frac{\mu^2(k)}{f(k)}} + \sum_{1 \leqslant k_1, k_2 \leqslant \xi} \lambda_{k_1} \lambda_{k_2} R\left\{\frac{k_1 k_2}{(k_1, k_2)}\right\},$$

此處

$$f(k)=\sum_{d|k}\mu(d)\Big/g\left(\frac{k}{d}\right)^{*},\tag{4}$$

$$\lambda_k=\frac{\mu(k)}{f(k)\,g(k)}\sum_{\substack{1\leqslant m\leqslant\xi/k\\(m,k)=1}}\frac{\mu^2(m)}{f(m)}\Big/\sum_{1\leqslant m\leqslant\xi}\frac{\mu^2(m)}{f(m)}.\tag{5}$$

證：令 $1=\lambda_1,\lambda_2,\cdots,\lambda_{[\xi]}$ 爲實數．因 k_1,k_2 之最小公倍數爲 $\frac{k_1k_2}{(k_1,k_2)}$，由 (3) 得

$$N_\xi=\sum_{p|b\Rightarrow p>\xi}{}_b\,1=\sum_{p|b\Rightarrow p>\xi}{}_b\,1\Big(\sum_{\substack{k|b\\1\leqslant k\leqslant\xi}}\lambda_k\Big)^2\leqslant\sum_b\Big(\sum_{\substack{k|b\\1\leqslant k\leqslant\xi}}\lambda_k\Big)^2=$$

$$=\sum_{1\leqslant k_1,k_2\leqslant\xi}\lambda_{k_1}\lambda_{k_2}\sum_{\substack{k_1|b\\k_2|b}}{}_b\,1=\sum_{1\leqslant k_1,k_2\leqslant\xi}\lambda_{k_1}\lambda_{k_2}\sum_{\frac{k_1k_2}{(k_1,k_2)}\Big|b}{}_b\,1=$$

$$=\sum_{1\leqslant k_1,k_2\leqslant\xi}\lambda_{k_1}\lambda_{k_2}\left(g\left\{\frac{k_1k_2}{(k_1,k_2)}\right\}M+R\left\{\frac{k_1k_2}{(k_1,k_2)}\right\}\right),$$

此處 $p|b\Rightarrow p>\xi$ 表示 b 的素因子皆大於 ξ，由定理 6.2.4，有

$$N_\xi\leqslant MQ+\sum_{1\leqslant k_1,k_2\leqslant\xi}\lambda_{k_1}\lambda_{k_2}R\left\{\frac{k_1k_2}{k_1,k_2}\right\},\tag{6}$$

此處

$$Q=\sum_{1\leqslant k_1,k_2\leqslant\xi}\lambda_{k_1}\lambda_{k_2}\frac{g(k_1)\,g(k_2)}{g\{(k_1,k_2)\}}.$$

由 (4) 及定理 6.4.1，有

$$Q=\sum_{1\leqslant k_1,k_2\leqslant\xi}\lambda_{k_1}\lambda_{k_2}g(k_1)\,g(k_2)\sum_{d|(k_1,k_2)}f(d)=$$

$$=\sum_{1\leqslant d\leqslant\xi}f(d)\sum_{\substack{1\leqslant k_1\leqslant\xi\\d|k_1}}\lambda_{k_1}g(k_1)\sum_{\substack{1\leqslant k_2\leqslant\xi\\d|k_2}}\lambda_{k_2}g(k_2)=$$

$$=\sum_{1\leqslant d\leqslant\xi}f(d)\Big\{\sum_{\substack{1\leqslant k\leqslant\xi\\d|k}}\lambda_k g(k)\Big\}^2.\tag{7}$$

由 (5) 及定理 6.2.1 可知 $\lambda_1=1$．(如此選擇的 $\lambda_1,\cdots,\lambda_{[\xi]}$，使 Q 最小，讀者可用定理 1 自證之)．

*當 k 無平方因子時，$f(k)=\frac{1}{g(k)}\prod_{p|k}(1-g(p))>0$.

令

$$s=\sum_{1\leqslant m\leqslant\xi}\frac{\mu^2(m)}{f(m)}. \tag{8}$$

由定理 6.2.2, 可知 $f(n)$ 也是積性的,故由 (5) 得

$$\lambda_k g(k)=\frac{\mu(k)}{sf(k)}\sum_{\substack{1\leqslant m\leqslant\xi/k\\(m,k)=1}}\frac{\mu^2(m)}{f(m)}=\sum_{\substack{1\leqslant m\leqslant\xi/k\\(m,k)=1}}\mu(m)\frac{\mu(mk)}{sf(mk)}=$$

$$=\sum_{1\leqslant m\leqslant\xi/k}\mu(m)\frac{\mu(mk)}{sf(mk)}.$$

由定理 6.3.2, 有

$$\frac{\mu(m)}{sf(m)}=\sum_{1\leqslant k\leqslant\xi/m}\lambda_{km}g(km)=\sum_{\substack{1\leqslant r\leqslant\xi\\m|r}}\lambda_r g(r).$$

因此,由 (7),(8) 有

$$Q=\sum_{1\leqslant d\leqslant\xi}f(d)\left\{\frac{\mu(d)}{sf(d)}\right\}^2=\frac{1}{s^2}\sum_{1\leqslant d\leqslant\xi}\frac{\mu^2(d)}{f(d)}=\frac{s}{s^2}=\frac{1}{s}.$$

於是,由 (6),(8),定理已明.

定理 3. 在定理 2 的條件下,若 $g_1(n)$ 爲完全積性函數,且 $g_1(p)=g(p)$, 則

$$N_\xi\leqslant\frac{M}{\sum_{1\leqslant k\leqslant\xi}g_1(k)}+$$

$$+\sum_{1\leqslant k_1,k_2\leqslant\xi}\left|R\left\{\frac{k_1k_2}{(k_1,k_2)}\right\}\right|\prod_{p|k_1}\{1-g_1(p)\}^{-1}\prod_{p|k_2}\{1-g_1(p)\}^{-1}.$$

在證明定理 3 之前,需要先證明下列之定理:

定理 4. 若 $f(n)$ 爲一完全積性函數,且 $0\leqslant f(p)<1$. β_n 爲一組實數, 且 $\beta_n\geqslant 0$, 則

$$\sum_{1\leqslant n\leqslant\xi}\beta_n f(n)\prod_{p|k_n}\{1-f(p)\}^{-1}\geqslant\sum_{1\leqslant n\leqslant\xi}f(n)\sum_{\substack{m|n\\p|\frac{n}{m}\Rightarrow p|k_m}}\beta_m,$$

此處 $p\left|\frac{n}{m}\Rightarrow p\right|k_m$ 表示 $\frac{n}{m}$ 中只含有 k_m 的素因子.

證:
$$\sum_{1\le n\le \xi}\beta_n f(n)\prod_{p|k_n}\{1-f(p)\}^{-1}=\sum_{1\le n\le \xi}\beta_n f(n)\prod_{p|k_n}\sum_{m=0}^{\infty}\{f(p)\}^m=$$
$$=\sum_{1\le n\le \xi}\beta_n f(n)\prod_{p|k_n}\sum_{m=0}^{\infty}f(p^m)=\sum_{1\le n\le \xi}\beta_n f(n)\sum_{\substack{r=1\\ p|r\to p|k_n}}^{\infty}f(r)=$$
$$=\sum_{1\le n\le \xi}\beta_n\sum_{\substack{r=1\\ p|r\to p|k_n}}^{\infty}f(nr)=\sum_{1\le n\le \xi}\beta_n\sum_{\substack{s=1\\ n|s\\ p|\frac{s}{n}\to p|k_n}}^{\infty}f(s)=$$
$$=\sum_{s=1}^{\infty}f(s)\sum_{\substack{1\le n\le \xi\\ n|s\\ p|\frac{s}{n}\to p|k_n}}\beta_n\geqslant\sum_{1\le s\le \xi}f(s)\sum_{\substack{1\le n\le \xi\\ n|s\\ p|\frac{s}{n}\to p|k_n}}\beta_n=$$
$$=\sum_{1\le s\le \xi}f(s)\sum_{\substack{n|s\\ p|\frac{s}{n}\to p|k_n}}\beta_n.$$

定理已明.

定理 3 之證明: 由 (4), 有
$$f(p)=\frac{\mu(1)}{g(p)}+\frac{\mu(p)}{g(1)}=\frac{1}{g(p)}-1=\frac{1-g(p)}{g(p)}.$$

由定理 6.2.2, 若 k 無平方因子,則
$$\frac{\mu^2(k)}{f(k)}=\mu^2(k)\prod_{p|k}\frac{g_1(p)}{1-g_1(p)}=\mu^2(k)\frac{\prod_{p|k}g_1(p)}{\prod_{p|k}\{1-g_1(p)\}}=$$
$$=\mu^2(k)\,g_1(k)\prod_{p|k}\{1-g_1(p)\}^{-1}. \tag{9}$$

上面的關係式當 $k=1$ 及 k 有平方因子時亦成立. 因此,由定理 4, 有
$$\sum_{1\le k\le \xi}\frac{\mu^2(k)}{f(k)}=\sum_{1\le k\le \xi}\mu^2(k)\,g_1(k)\prod_{p|k}\{1-g_1(p)\}^{-1}\geqslant$$
$$\geqslant\sum_{1\le k\le \xi}g_1(k)\sum_{\substack{m|k\\ p|\frac{k}{m}\to p|m}}\mu^2(m).$$

命 d_k 表 k 的最大的無平方因子的除數,則 $d_k|k$. 若 $p\left|\frac{k}{d_k}\right.$,則 $p|k$, 因而

$p|d_k$. 故 d_k 爲適合條件之 m, 卽得

$$\sum_{1\leqslant k\leqslant\xi}\frac{\mu^2(k)}{f(k)}\geqslant\sum_{1\leqslant k\leqslant\xi}g_1(k).\tag{10}$$

由 (9), 易見 $\mu^2(k)/f(k)\geqslant 0$. 則由 (5), (9) 可知

$$|\lambda_k|\leqslant\frac{\mu^2(k)}{f(k)\,g(k)}=\frac{\mu^2(k)}{f(k)\,g_1(k)}\leqslant\prod_{p|k}\{1-g_1(p)\}^{-1},$$

蓋因當 $k=1$ 及 k 無平方因子時 $g(k)=g_1(k)$, 而 k 有平方因子時 $\mu(k)=0$ 故也. 由此及 (10), 利用定理 2 卽得本定理.

定理 5. 命 $A\geqslant 0$, $M\geqslant 3$. 記在 A 與 $A+M$ 間的素數個數爲 $\pi(A;M)$. 則

$$\pi(A;M)\leqslant\frac{2M}{\log M}\left(1+O\left(\frac{\log\log M}{\log M}\right)\right).$$

此處與 O 有關之常數與 A 及 M 無關.

證: 由於

$$\pi(A;M)=\sum_{A<p\leqslant A+M^{\frac{1}{2}}}1+\sum_{A+M^{\frac{1}{2}}<p\leqslant A+M}1\leqslant M^{\frac{1}{2}}+S(A;M).\tag{11}$$

現在取整數集合 $\{b\}$ 爲適合 $A<n\leqslant A+M$ 的全體整數. 用定理 3 的記號可知

$$S(A;M)\leqslant N_\xi,\qquad 1<\xi\leqslant\sqrt{M}\tag{12}$$

對所有的 $A\geqslant 0$ 皆成立. 現在來估計 N_ξ. 因爲

$$\sum_{\substack{k|b\\A<b\leqslant A+M}}1=\left[\frac{A+M}{k}\right]-\left[\frac{A}{k}\right]=\frac{M}{k}+R(k),\qquad |R(k)|\leqslant 1.$$

故 $g_1(k)=\dfrac{1}{k}$. 因此

$$\sum_{1\leqslant k\leqslant\xi}g_1(k)=\log\xi+O(1).$$

由定理 5.9.3 可知

$$\prod_{p|k}(1-g_1(p))^{-1}=\prod_{p|k}\left(1-\frac{1}{p}\right)^{-1}\leqslant\prod_{p\leqslant k}\left(1-\frac{1}{p}\right)^{-1}=O(\log k).$$

故

$$\sum_{1\leqslant k_1,k_2\leqslant\xi}\left|R\left(\frac{k_1k_2}{(k_1,k_2)}\right)\right|\prod_{p|k_1}(1-g_1(p))^{-1}\prod_{p|k_2}(1-g_1(p))^{-1}=$$

$$= O\Big(\sum_{1 \leqslant k_1, k_2 \leqslant \xi} \log k_1 \log k_2\Big) = O(\xi^2 \log^2 \xi).$$

故

$$N_\xi \leqslant \frac{M}{\log \xi + O(1)} + O(\xi^2 \log^2 \xi).$$

取

$$\xi = M^{\frac{1}{2}} / \log^2 M,$$

則得

$$N_{M^{\frac{1}{2}}/\log^2 M} \leqslant \frac{2M}{\log M}\Big(1 + O\Big(\frac{\log\log M}{\log M}\Big)\Big).$$

以此代入 (11), (12), 卽明所欲證.

§5. Гольдбах–Шнирельман 定理之證明.

定理 1. 若 $a \geqslant 2$, 則

$$r(a) \leqslant c_5 \frac{a}{\log^2 a} \sum_{k|a} \frac{\mu^2(k)}{k}.$$

證: $a = 2$ 或 $a = 3$ 時, 因爲 $r(a) = 0$, 定理已成立. 又若 a 是奇數, 而 $p_1 + p_2 = a$, 則必 $p_1 = 2$ 或 $p_2 = 2$. 此時 $r(a) \leqslant 2$. 定理顯然成立.

以下設 $a \geqslant 4$ 且爲偶數. 易得

$$r(a) = \sum_{p_1+p_2=a} 1 \leqslant \sum_{\substack{p_1+p_2=a \\ p_1, p_2 > \sqrt{a}}} 1 + \sum_{\substack{p_1+p_2=a \\ p_1 \leqslant \sqrt{a}}} 1 + \sum_{\substack{p_1+p_2=a \\ p_2 \leqslant \sqrt{a}}} 1 \leqslant S(a) + 2\sqrt{a}, \qquad (1)$$

此處

$$S(a) = \sum_{\substack{p_1+p_2=a \\ p_1, p_2 > \sqrt{a}}} 1.$$

現在給一整數集合 $b_c = c(a-c)$ $(c = 1, 2, \cdots, a)$. 若 $p_1 + p_2 = a$ 而 $p_1, p_2 > \sqrt{a}$, 則 $p_1(a-p_1) = p_2(a-p_2) = p_1 p_2$ 不能被 $\leqslant \sqrt{a}$ 的素數所整除. 若用 §4 的記號, 則得

$$S(a) \leqslant N_\xi, \quad 1 < \xi \leqslant \sqrt{a}. \qquad (2)$$

命 $M(k)$ 表示同餘式 $x(a-x) \equiv 0 \pmod{k}$ $(0 \leqslant x < k)$ 的解數, 則

$$\sum_{k|b} 1 = \sum_{\substack{c=1 \\ c(a-c) \equiv 0 \ (\mathrm{mod}\ k)}}^{a} 1 = \Big[\frac{a}{k}\Big] M(k) + T(k),$$

此處 $0 \leqslant T(k) \leqslant M(k)$. 故得

$$\sum_{k|b} 1 \leqslant \frac{M(k)}{k} a + M(k)$$

及

$$\sum_{k|b} 1 \geqslant \left[\frac{a}{k}\right] M(k) > \left(\frac{a}{k} - 1\right) M(k) = \frac{M(k)}{k} a - M(k).$$

命

$$g(k) = \frac{M(k)}{k}, \tag{3}$$

則

$$\sum_{k|b} 1 = g(k)\, a + R(k), \tag{4}$$

此處

$$|R(k)| \leqslant M(k) \leqslant k. \tag{5}$$

由定理 2.8.1 知 $M(k)$ 是 k 的積性函數,故 $g(k)$ 亦然. 又

$$M(p) = \begin{cases} 1, & p|a, \\ 2, & p \nmid a. \end{cases} \tag{6}$$

故由 (3) 得

$$g_1(p) = g(p) = \begin{cases} \frac{1}{p}, & p|a, \\ \frac{2}{p}, & p \nmid a. \end{cases} \tag{7}$$

因爲 $2|a$, 故 $g(2) = \frac{1}{2}$; 因此 $0 < g(p) < 1$, 故可應用定理 4.3, 若 $k = p_1^{a_1} \cdots p_r^{a_r}$, 則由 (3) 及 (6) 式得

$$g_1(k) = \prod_{s=1}^{r} \{g_1(p_s)\}^{a_s} = \prod_{s=1}^{r} \frac{\{M(p_s)\}^{a_s}}{p_s^{a_s}} = \frac{1}{k} \prod_{\substack{s=1 \\ p_s \nmid a}}^{r} 2^{a_s} \geqslant$$

$$\geqslant \frac{1}{k} \prod_{\substack{s=1 \\ p_s \nmid a}}^{r} (1 + a_s) = \frac{h(k)}{k},$$

此處

$$h(p_1^{a_1} \cdots p_r^{a_r}) = \prod_{\substack{s=1 \\ p_s \nmid a}}^{r} (1 + a_s), \qquad p_1, \cdots, p_r \text{ 爲不同的素數}. \tag{8}$$

由定理 4.4 得

$$\prod_{p|a}\left(1-\frac{1}{p}\right)^{-1}\sum_{1\leqslant k\leqslant\xi} g_1(k)\geqslant\sum_{1\leqslant k\leqslant\xi} h(k)\frac{1}{k}\prod_{p|a}\left(1-\frac{1}{p}\right)^{-1}\geqslant$$

$$\geqslant\sum_{1\leqslant k\leqslant\xi}\frac{1}{k}\sum_{\substack{m|k\\ p|\frac{k}{m}\Rightarrow p|a}} h(m).$$

若書 k 爲 $k=p_1^{a_1}\cdots p_t^{a_t}q_1^{b_1}\cdots q_u^{b_u}$，其中諸 p_T 與 q_U 均爲互不相同的素數，且 $p_T|a$，$q_U\nmid a$. 則 m 可取所有如下形式的整數：

$$m=\frac{k}{p_1^{c_1}\cdots p_t^{c_t}}=p_1^{a_1-c_1}\cdots p_t^{a_t-c_t}q_1^{b_1}\cdots q_u^{b_u},$$

其中 $0\leqslant c_1\leqslant a_1,\cdots,0\leqslant c_t\leqslant a_t$. 對於這種 m，由 (8) 知

$$h(m)=(1+b_1)\cdots(1+b_u).$$

故由習題 6.5.1 得

$$\prod_{p|a}\left(1-\frac{1}{p}\right)^{-1}\sum_{1\leqslant k\leqslant\xi} g_1(k)\geqslant\sum_{1\leqslant k\leqslant\xi}\frac{1}{k}\sum_{c_1=0}^{a_1}\cdots\sum_{c_t=0}^{a_t}(1+b_1)\cdots(1+b_u)=$$

$$=\sum_{1\leqslant k\leqslant\xi}\frac{1}{k}(1+a_1)\cdots(1+a_t)(1+b_1)\cdots(1+b_u)=$$

$$=\sum_{1\leqslant k\leqslant\xi}\frac{d(k)}{k}\geqslant c_6\log^2\xi.$$

故

$$\sum_{1\leqslant k\leqslant\xi} g_1(k)\geqslant c_6\log^2\xi\prod_{p|a}\left(1-\frac{1}{p}\right)=c_6\log^2\xi\prod_{p|a}\left(1-\frac{1}{p^2}\right)\prod_{p|a}\left(1+\frac{1}{p}\right)^{-1}\geqslant$$

$$\geqslant c_6\log^2\xi\prod_{p}\left(1-\frac{1}{p^2}\right)\prod_{p|a}\left(1+\frac{1}{p}\right)^{-1}\geqslant$$

$$\geqslant c_7\log^2\xi\left\{\sum_{k|a}\frac{\mu^2(k)}{k}\right\}^{-1}. \tag{9}$$

其次，若 $k=\prod_{p|k}p^c$. 則由

$$\prod_{p|k}\{1-g_1(p)\}^{-1}\leqslant\{1-g_1(2)\}^{-1}\{1-g_1(3)\}^{-1}\prod_{5\leqslant p|k}\{1-g_1(p)\}^{-1}\leqslant$$

$$\leqslant 2\cdot 3\prod_{5\leqslant p|k}\left(1-\frac{2}{5}\right)^{-1}<6\prod_{p|k}(1+c)=6\,d(k)\leqslant 6k.$$

故由定理 4.3, (5) 及 (9) 得

$$S(a) \leqslant N_\xi \leqslant \frac{1}{c_7} \cdot \frac{a}{\log^2 \xi} \sum_{k|a} \frac{\mu^2(k)}{k} + \sum_{1 \leqslant k_1, k_2 \leqslant \xi} \frac{k_1 k_2}{(k_1, k_2)} 6 k_1 \cdot 6 k_2 \leqslant$$

$$\leqslant \frac{1}{c_7} \cdot \frac{a}{\log^2 \xi} \sum_{k|a} \frac{\mu^2(k)}{k} + 36 \xi^6 .$$

取 $\xi = a^{1/10}$, 由 (1) 式卽得定理。

定理 3.4 之證明: $n \geqslant 2$ 時,有

$$\sum_{1 \leqslant a \leqslant n} r^2(a) \leqslant 1 + \sum_{4 \leqslant a \leqslant n} c_5^2 \frac{a^2}{\log^4 a} \sum_{k_1|a} \frac{\mu^2(k_1)}{k_1} \sum_{k_2|a} \frac{\mu^2(k_2)}{k_2} \leqslant$$

$$\leqslant 1 + c_5^2 \frac{n^2}{\log^4 n} \sum_{4 \leqslant a \leqslant n} \sum_{\substack{k_1|a \\ k_2|a}} \frac{1}{k_1 k_2} \leqslant$$

$$\leqslant 1 + c_5^2 \frac{n^2}{\log^4 n} \sum_{1 \leqslant k_1, k_2 \leqslant n} \frac{1}{k_1 k_2} \sum_{\substack{1 \leqslant a \leqslant n \\ \frac{k_1 k_2}{(k_1, k_2)} \Big| a}} 1 \leqslant$$

$$\leqslant 1 + c_5^2 \frac{n^2}{\log^4 n} \sum_{1 \leqslant k_1, k_2 \leqslant n} \frac{1}{k_1 k_2} \cdot \frac{n}{\frac{k_1 k_2}{(k_1, k_2)}} .$$

因爲 $(k_1, k_2) \leqslant \min\{k_1, k_2\} \leqslant \sqrt{k_1 k_2}$, 故

$$\sum_{1 \leqslant a \leqslant n} r^2(a) \leqslant 1 + c_5^2 \frac{n^2}{\log^4 n} \sum_{1 \leqslant k_1, k_2 \leqslant n} \frac{n}{(k_1 k_2)^{3/2}} \leqslant$$

$$\leqslant 1 + c_5^2 \frac{n^3}{\log^4 n} \left(\sum_{k=1}^{\infty} \frac{1}{k^{3/2}} \right)^2 \leqslant$$

$$\leqslant c_4 \frac{n^3}{\log^4 n} .$$

卽得定理。

習題 1. 設 x, k, l 都是正整數, 且 $(k, l) = 1$. $\pi(x; k, l)$ 表示算術級數 $a_n = kn + l$ $(n = 1, 2, \cdots)$ 所包含的不超過 x 的素數的個數, 又命 δ 是滿足 $0 < \delta < 1$ 的固定常數,求證當 $k < x^\delta$ 時,有

$$\pi(x; k, l) \leqslant \frac{2x}{\varphi(k) \log \frac{x}{k}} \left(1 + O\left(\frac{(\log \log x)^2}{\log x} \right) \right),$$

此處 O 中所含之常數與 k 無關,但與 δ 有關.

習題 2. 若 $p, p+2$ 同時爲素數,則 p 與 $p+2$ 就稱做一對"孿生素數". 以 $Z_2(N)$ 表示小於或等於 N 的"孿生素數"的對數. 則

$$Z_2(N) \leqslant c_8 \frac{N}{\log^2 N};$$

並證明級數

$$\sum_{p^*} \frac{1}{p^*}$$

收斂,此處 p^* 經過所有的"孿生素數", 卽 p^* 與 p^*-2 是一對"孿生素數".

§ 6. Waring-Hilbert 定理.

在 §§6—7 中, $c, c_1, c_2, \cdots$ 皆表僅與 k 有關之正常數. 與 O 有關之常數亦僅與 k 有關. §§6—7 之目的在於證明

定理 1 (Hilbert). 對任一整數 $k(\geqslant 1)$, 有一正整數 c 存在, 凡正整數必爲不多於 c 個正整數之 k 乘方和.

今定義 $\mathfrak{A}_t^*$ 爲整數

$$x_1^k + \cdots + x_t^k$$

所成之集合,此處 x_m 各過所有的非負整數. 定義 $\mathfrak{A}_t$ 爲 $\mathfrak{A}_t^*$ 中不同元素所成之最大分集合. 命

$$c_1 = c_1(k) = \frac{1}{2} 8^{k-1}.$$

證明之環節在證明:

定理 2. 若 $k \geqslant 2$, 則 $\mathfrak{A}_{c_1}$ 有正密率.

由定理 2.3 可知定理 1 可由定理 2 直接推得.

定義 $r(a)$ 爲不定方程

$$x_1^k + \cdots + x_{c_1}^k = a, \qquad x_m \geqslant 0$$

之解數. 今先證明:

定理 3. 若 $n \geqslant 1$, 則

$$\sum_{1 \leqslant a \leqslant n} r(a) \geqslant c_2(k)\, n^{c_1/k}.$$

證：顯然可假定 $n > c_1$．有

$$\sum_{1\leqslant a\leqslant n} r(a) = -1 + \sum_{0\leqslant a\leqslant n} \sum_{\substack{x_1^k+\cdots+x_{c_1}^k=a\\ x_m\geqslant 0}} 1 \geqslant$$

$$\geqslant -1 + \sum_{0\leqslant x_1\leqslant (n/c_1)^{1/k}} \cdots \sum_{0\leqslant x_{c_1}\leqslant (n/c_1)^{1/k}} 1 \geqslant$$

$$\geqslant \left(\frac{n}{c_1}\right)^{c_1/k} - 1 \geqslant c_3(k)\, n^{c_1/k}.$$

由定理 3 及定理 2.4 可知，中心環節在於證明：

定理 4. 若 $k\geqslant 2$ 及 $n\geqslant 1$，則

$$\sum_{1\leqslant a\leqslant n} r^2(a) \leqslant c_4(k)\, n^{2c_1/k-1}.$$

蓋若此定理證明，則由定理 2.4 及定理 3 卽可得出定理 2 矣．

今將定理 4 略變其形式．

定理 5. 若 $k\geqslant 2$ 及 $P\geqslant 1$，則

$$\int_0^1 \left| \sum_{x=0}^{P} e^{2\pi i x^k \alpha} \right|^{2c_1} d\alpha \leqslant c_5(k)\, P^{2c_1-k}.$$

取 $P=[n^{1/k}]$，顯然當 n 大時，$c_1 P^k > n$．

習知，對一整數 q

$$\int_0^1 e^{2\pi i q\alpha}\, d\alpha = \begin{cases} 1, & \text{若 } q=0, \\ 0, & \text{若 } q\neq 0. \end{cases}$$

由定理 5 得出

$$\sum_{1\leqslant a\leqslant n} r^2(a) \leqslant \sum_{0\leqslant a\leqslant c_1P^k} \Bigg(\sum_{\substack{x_1^k+\cdots+x_{c_1}^k=a\\ 0\leqslant x_i\leqslant P\\ 1\leqslant i\leqslant c_1}} 1 \Bigg)^2 =$$

$$= \int_0^1 \Bigg| \sum_{0\leqslant a\leqslant c_1P^k} e^{2\pi i a\alpha} \sum_{\substack{x_1^k+\cdots+x_{c_1}^k=a\\ 0\leqslant x_i\leqslant P\\ 1\leqslant i\leqslant c_1}} 1 \Bigg|^2 d\alpha =$$

$$= \int_0^1 \left| \sum_{x_1=0}^{P} \cdots \sum_{x_{c_1}=0}^{P} e^{2\pi i (x_1^k+\cdots+x_{c_1}^k)\alpha} \right|^2 d\alpha =$$

$$= \int_0^1 \left| \sum_{x=0}^{P} e^{2\pi i x^k \alpha} \right|^{2c_1} d\alpha \leqslant c_5(k) P^{2c_1-k} \leqslant$$

$$\leqslant c_4(k) n^{2c_1/k-1}.$$

此卽定理 4.

因此今後之目的在於證明定理 5.

習題. 從定理 4 推出定理 5.

§ 7. Waring-Hilbert 定理的證明.

定理 1. 若 $X, Y \geqslant 1$, n 爲一整數, $q(n)$ 表示方程

$$x_1 y_1 + x_2 y_2 = n \qquad (|x_m| \leqslant X, \quad |y_m| \leqslant Y, \quad m = 1, 2) \tag{1}$$

的整數解數,則

$$q(n) \leqslant \begin{cases} 27\, X^{3/2}\, Y^{3/2}, & \text{若} \quad n = 0; \\ 60\, XY \sum_{d|n} \dfrac{1}{d}, & \text{若} \quad n \neq 0. \end{cases} \tag{2}$$

證: 1) $n = 0$; 此時 x_1, x_2, y_1 所能取之值分別不超過 $2X+1$, $2X+1$ 及 $2Y+1$. 當 x_1, x_2, y_1 確定之後, y_2 最多只能够取一個值, 故

$$q(0) \leqslant (2X+1)^2 (2Y+1) \leqslant (3X)^2 (3Y) = 27\, X^2\, Y.$$

同法可得

$$q(0) \leqslant 27\, XY^2.$$

故

$$q(0) \leqslant \min(27\, X^2 Y, \ 27\, XY^2) \leqslant \sqrt{27\, X^2 Y \cdot 27\, XY^2} = 27\, X^{3/2}\, Y^{3/2}.$$

2) $n \neq 0$; 不失一般性,可以假定 $X \leqslant Y$. 設 $q_1(n)$ 是方程

$$x_1 y_1 + x_2 y_2 = n \quad ((x_1, x_2) = 1, \quad |x_2| \leqslant |x_1| \leqslant X, \quad |y_m| \leqslant Y, \quad m = 1, 2). \tag{3}$$

的整數解數. 易知 $x_1 \neq 0$, 否則 $x_2 = 0$, 則 $n = 0$ 矣. 此與假定相矛盾. 又命 $q_2(n; x_1, x_2)$ 表示對於一組固定的 x_1, x_2, 而 $(x_1, x_2) = 1$, $|x_2| \leqslant |x_1| \leqslant X$, 方程 (3) 對 y_1, y_2 的整數解數. 由定理 1.8.2 知此時 (3) 式可解. 且若 y_1', y_2' 是其一組解,則其他的解 y_1, y_2 可以表成

$$y_1 = y_1' + t x_2, \qquad y_2 = y_2' - t x_1, \qquad t \text{ 爲整數}.$$

故

$$|t| = \left|\frac{y_2'-y_2}{x_1}\right| \leqslant \frac{Y+Y}{|x_1|} = \frac{2Y}{|x_1|}.$$

故 t 可取之值不超過 $2\cdot\frac{2Y}{|x_1|}+1 \leqslant \frac{4Y+X}{|x_1|} \leqslant \frac{5Y}{|x_1|}$，即

$$q_2(n; x_1, x_2) \leqslant \frac{5Y}{|x_1|}.$$

故

$$q_1(n) \leqslant \sum_{1\leqslant|x_1|\leqslant X}\ \sum_{|x_2|\leqslant|x_1|} \frac{5Y}{|x_1|} \leqslant 5Y \sum_{1\leqslant|x_1|\leqslant X} \frac{2|x_1|+1}{|x_1|} \leqslant$$

$$\leqslant 5Y\cdot 3\cdot 2X = 30\,XY.$$

因此滿足條件 $(x_1, x_2)=1$ 之方程式 (1) 之解數不超過 $2\cdot 30XY = 60\,XY$.

其次，若 $(x_1, x_2) = d \neq 1$, $d|n$，則命 $\frac{x_1}{d} = x_1'$, $\frac{x_2}{d} = x_2'$ 此時即要求方程

$$x_1' y_1 + x_2' y_1 = \frac{n}{d} \quad \left(|x_m'| \leqslant \frac{X}{d},\quad |y_m| \leqslant Y,\quad m=1,2,\quad (x_1', x_2')=1\right)$$

的整數解數，由上述知其解數不超過 $60\frac{X}{d}\cdot Y$.

故當 $n \neq 0$ 時得

$$q(n) \leqslant 60\,XY \sum_{d|n} \frac{1}{d}.$$

定理證畢.

定理 6.5 顯然是下面定理的推論.

定理 2. 若 $k \geqslant 2$, $f(x)$ 爲一個 k 次整係數多項式

$$f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0,$$

$$a_k = O(1),\ a_{k-1} = O(P),\ \cdots,\ a_1 = O(P^{k-1}),\quad a_0 = O(P^k),$$

則

$$\int_0^1 \left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^{8^{k-1}} d\alpha = O(P^{8^{k-1}-k}). \tag{4}$$

證: $k=2$ 時，(4) 之左端乃方程

$$f(x_1)+f(x_2)-f(y_1)-f(y_2) = f(x_3)+f(x_4)-f(y_3)-f(y_4)$$

$$(f(x) = a_2 x^2 + a_1 x + a_0,\quad a_2 = O(1),\quad a_1 = O(P),\quad a_0 = O(P^2)), \tag{5}$$

$$0 \leqslant x_m, y_m \leqslant P,\quad 1 \leqslant m \leqslant 4$$

的整數解數. 命 $x_i - y_i = z_i$, $a_2(x_i + y_i) + a_1 = w_i$ $(1 \leqslant i \leqslant 4)$. 可知 (5) 的解數不超過方程

$$z_1 w_1 + z_2 w_2 = z_3 w_3 + z_4 w_4 \quad (z_i = O(P),\ w_i = O(P),\ 1 \leqslant i \leqslant 4) \tag{6}$$

的整數解數. 若以 $q(n)$ 表示方程

$$z_1 w_1 + z_2 w_2 = n$$

$(z_i = O(P),\ w_i = O(P),\ m = 1, 2$, 此處與 O 有關之常數與 (6) 式相同) 的整數解數, 則立得 (6) 的解數爲 $\sum_{|n| \leqslant c_6 P^2} q(n)^2$. 由定理 1 可知

$$\sum_{|n| \leqslant c_6 P^2} q(n)^2 = O(P^6) + O\left(\sum_{1 \leqslant n \leqslant c_6 P^2} \left(P^2 \sum_{d|n} \frac{1}{d} \right)^2 \right) =$$

$$= O(P^6) + O\left(P^4 \sum_{1 \leqslant d_1,\ d_2 \leqslant c_6 P^2} \frac{1}{d_1 d_2} \sum_{\substack{\frac{d_1 d_2}{(d_1, d_2)} \Big| n \\ 1 \leqslant n \leqslant c_6 P^2}} 1 \right) =$$

$$= O(P^6) + O\left(P^4 \sum_{d_1=1}^{\infty} \sum_{d_2=1}^{\infty} \frac{P^2}{(d_1 d_2)^{3/2}} \right) =$$

$$= O(P^6).$$

定理成立.

現在假定 $k \geqslant 3$. 由歸納法,假定 $k-1$ 時定理已眞. 由於

$$\left| \sum_{x=0}^{P} e^{2\pi i f(x) \alpha} \right|^2 = \sum_{x=0}^{P} e^{-2\pi i f(x) \alpha} \sum_{-x \leqslant h \leqslant P-x} e^{2\pi i f(x+h) \alpha} =$$

$$= \sum_{0 < |h| \leqslant P}{}' \sum_{x=0}^{P}{}' e^{2\pi i h \varphi(x, h) \alpha} + P, \tag{7}$$

此處 Σ' 表示過所示區間內整數的某一部分集合, 而 $\varphi(x, h) = \frac{1}{h}(f(x+h) - f(x))$, $(h \neq 0)$, 把 $\varphi(x, h)$ 看成變數 x 的多項式時,可知 $\varphi(x, h)$ 乃是適合定理要求的 $k-1$ 次多項式. 記 $a_h = \sum_{x=0}^{P}{}' e^{2\pi i h \varphi(x, h) \alpha}$, 則

$$\left| \sum_{x=0}^{P} e^{2\pi i f(x) \alpha} \right|^{2 \cdot 8^{k-2}} \leqslant 2^{8^{k-2}} \max\left(\left| \sum_{0 < |h| \leqslant P}{}' a_h \right|^{8^{k-2}},\ P^{8^{k-2}} \right).$$

若 $\left| \sum_{0 < |h| \leqslant P}{}' a_h \right| \leqslant P$, 則定理顯然成立. 否則,連續運用 Буняковский–Schwarz 不等式,得

$$2^{-8^{k-2}}\left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^{2\cdot 8^{k-2}} \leqslant \left|\sum_{0<|h|\leqslant P}{}' a_h\right|^{8^{k-2}} \leqslant \left\{\sum_{0<|h|\leqslant P}{}' 1\cdot \sum_{0<|h|\leqslant P}{}' |a_h|^2\right\}^{2^{3(k-2)-1}} \leqslant$$

$$\leqslant \left\{\left(\sum_{0<|h|\leqslant P}{}' 1\right)^{2^2-1}\sum_{0<|h|\leqslant P}{}' |a_h|^{2^2}\right\}^{2^{3(k-2)-2}} \leqslant\cdots\leqslant$$

$$\leqslant \left\{\left(\sum_{0<|h|\leqslant P}{}' 1\right)^{2^{3(k-2)-1}-1}\sum_{0<|h|\leqslant P}{}' |a_h|^{2^{3(k-2)-1}}\right\}^{2} \leqslant$$

$$\leqslant (3P)^{8^{k-2}-1}\sum_{0<|h|\leqslant P}{}' |a_h|^{8^{k-2}} = O\left(P^{8^{k-2}-1}\sum_{0<|h|\leqslant P}{}'\left|\sum_{x=0}^{P}{}' e^{2\pi i h\varphi(x,h)\alpha}\right|^{8^{k-2}}\right). \quad (8)$$

命

$$\left|\sum_{x=0}^{P}{}' e^{2\pi i h\varphi(x,h)\alpha}\right|^{8^{k-2}} = \sum_{n} A(n)e^{2\pi i h n\alpha}. \quad (9)$$

由於 $0\leqslant x\leqslant P$，可知 $n = O(\max\limits_{0\leqslant x\leqslant P}|\varphi(x,h)|) = O(P^{k-1})$. 由 (9) 及歸納法假定

$$|A(n)| = \left|\int_0^1 \left|\sum_{x=0}^{P}{}' e^{2\pi i\varphi(x,h)\beta}\right|^{8^{k-2}} e^{-2\pi i n\beta}\,d\beta\right| \leqslant$$

$$\leqslant \int_0^1 \left|\sum_{x=0}^{P} e^{2\pi i\varphi(x,h)\beta}\right|^{8^{k-2}} d\beta = O(P^{8^{k-2}-(k-1)}).$$

將 (8) 式 4 方後積分可知

$$\int_0^1 \left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^{8^{k-1}} d\alpha = O\left(P^{4\cdot 8^{k-2}-4}\int_0^1\left(\sum_{0<|h|\leqslant P}{}'\left|\sum_{x=0}^{P}{}' e^{2\pi i h\varphi(x,h)\alpha}\right|^{8^{k-2}}\right)^4 d\alpha\right) =$$

$$= O\left(P^{4\cdot 8^{k-2}-4}\sum_{\substack{n_1h_1+n_2h_2=n_3h_3+n_4h_4\\ 0<|h_i|\leqslant P\\ n_i=O(P^{k-1})\\ i=1,2,3,4}} A(n_1)A(n_2)A(n_3)A(n_4)\right) =$$

$$= O(P^{4\cdot 8^{k-2}-4}\cdot P^{3k}\cdot P^{4\cdot 8^{k-2}-4(k-1)}) = O(P^{8^{k-1}-k}).$$

定理證畢.

第 二 十 章

數 的 幾 何

§1. 二維空間之情況.

本節中將以二維空間爲例,概括地說明本章之基本內容.

定義 1. 命 c 表平面上之一簡單封閉曲線,此曲線範圍平面上之一部分 R,稱之爲域. 若域 R 中任意二點連線之中點恆在 R 中*, 則此域稱爲凸域.

例如: 圓、橢圓、平行四邊形、正 n 邊形皆爲凸域.

凸域之面積是存在的. (且可以定義爲: 在平面上打方格子,格子眼全在 R 中之小方塊面積之和之極限.)

本章將用及與凸域有關之若干概念及若干性質, 若欲與以嚴格說明,則必須有積分論及拓撲學之知識. 如讀者憑藉直觀,則了解本章之基本內容亦無困難. 特別是在應用時,所取的例子並不需要特殊的積分論或拓撲學之知識.

定理 1 (**Minkowski 基本定理**). 平面上一個以原點爲對稱中心之凸域 R, 其面積若大於 4, 則其中必包有異於原點之一整點. (整點者二坐標皆爲整數之點也.)

證 (Hajös): 以各偶整點 $(2r, 2s)$ 爲中心做邊長爲 2 之正方形 $S_{2r,2s}$. 若 $S_{2r,2s}$ 中有 R 之一部分,利用變形 $x-2r=x'$, $y-2s=y'$, 將此部分搬到正方形 $S_{0,0}$ 之中如此將 R 之所有部分皆集中到 $S_{0,0}$ 之中. 由於面積 >4, 故至少有二點重複. 假定此二點是由兩個不同的方塊 $S_{2r,2s}$, $S_{2r',2s'}$ 中搬來者. 原來此二點之坐標一定是

$$(x_0+2r,\ y_0+2s),\quad (x_0+2r',\ y_0+2s').$$

由於 R 以原點爲對稱中心,故

$$(-(x_0+2r'), -(y_0+2s'))$$

---

*由此不難得出,連任二點之線段必全部在 R 中.

也在 R 之中. 因爲 R 是凸域,二點 $(x_0+2r,\ y_0+2s)$ 及 $(-x_0-2r',\ -y_0-2s')$ 之中點

$$\left(\frac{x_0+2r-(x_0+2r')}{2},\ \frac{y_0+2s-(y_0+2s')}{2}\right)=(r-r',\ s-s')$$

仍在 R 之中,故得定理.

不難得出以下之結論:

定理 2. 若將定理 1 中的假定改爲面積 $\geqslant 4$, 則結論變爲:"所存在的異於原點之整點在 R 內或其邊上".

應用之一. 取 R 爲平行四邊形

$$|\xi|\leqslant b,\quad |\eta|\leqslant c, \tag{1}$$

此處

$$\xi=\alpha x+\beta y,\quad \eta=\gamma x+\delta y,\quad \alpha\delta-\beta\gamma=\Delta(\neq 0),$$

$\alpha, \beta, \gamma, \delta$ 是實數. (1) 定義一以原點爲對稱中心的平行四邊形,故爲凸域. 其面積等於

$$A=\iint\limits_{\substack{|\xi|\leqslant b\\|\eta|\leqslant c}} dx\,dy=\iint\limits_{\substack{|\xi|\leqslant b\\|\eta|\leqslant c}}\left|\frac{\partial(x,y)}{\partial(\xi,\eta)}\right| d\xi\,d\eta=\frac{1}{|\Delta|}\iint\limits_{\substack{|\xi|\leqslant b\\|\eta|\leqslant c}} d\xi\,d\eta=\frac{4bc}{|\Delta|}.$$

故若 $\frac{4bc}{|\Delta|}\geqslant 4$, 則有一非原點之整點適合於 (1). 即得:

定理 3. 若 $b>0,\ c>0,\ bc\geqslant|\Delta|$, 則必有一對整數 (x,y) $(\neq(0,0))$ 適合於 (1).

特別取 $\alpha=\delta=1,\ \gamma=0$, 則得一整數對 (x,y) $(\neq(0,0))$ 使

$$|x+\beta y|\leqslant b,\qquad |y|\leqslant\frac{1}{b},$$

即

$$\left|\beta+\frac{x}{y}\right|\leqslant\frac{b}{|y|}\leqslant\frac{1}{y^2}.$$

此即定理 6.10.6.

應用之二. 取 R 爲橢圓內部

$$\xi^2+\eta^2\leqslant r^2. \tag{2}$$

此顯然亦適合定理 1 之假定. (2) 之面積爲

$$\iint\limits_{\xi^2+\eta^2\leqslant r^2} dx\,dy = \iint\limits_{\xi^2+\eta^2\leqslant r^2} \left| \frac{\partial(x, y)}{\partial(\xi, \eta)} \right| d\xi\,d\eta = \frac{1}{|\Delta|} \iint\limits_{\xi^2+\eta^2\leqslant r^2} d\xi\,d\eta = \frac{\pi r^2}{|\Delta|}.$$

若 $\pi r^2 \geqslant 4|\Delta|$，則有一非原點之整點 (x, y) 適合於 (2). 由於任一以原點為中心的橢圓可以寫為

$$ax^2 + bxy + cy^2 = r^2, \tag{3}$$

命 $\xi = \sqrt{a}\,x + \frac{b}{2\sqrt{a}}\,y$ 及 $\eta = \sqrt{c - \frac{b^2}{4a}}\,y$，則 (3) 可以寫為 (2) 之形式，而

$$\Delta = \sqrt{ac - \left(\frac{b}{2}\right)^2}.$$

故得:

定理 4. 若 $a > 0$，$ac - \left(\frac{b}{2}\right)^2 > 0$，$\Delta = \sqrt{ac - \left(\frac{b}{2}\right)^2}$，則必有一整數對 $(x, y) \neq (0, 0)$ 使

$$ax^2 + bxy + cy^2 \leqslant \frac{4}{\pi}\Delta.$$

此結果並非最好，實則此 $\frac{4}{\pi}$ 可以 $\frac{2}{\sqrt{3}}$ 代之.

應用之三. 取 R 為雙曲線所範圍之域

$$|\xi\eta| \leqslant r^2. \tag{4}$$

此域不是凸域. 因此不能直接應用定理 1.2. 今之方法為在此域內做一凸域，使其面積 $\geqslant 4$. 今有

$$|\xi\eta| \leqslant \left(\frac{|\xi| + |\eta|}{2}\right)^2. \tag{5}$$

且

$$|\xi| + |\eta| \leqslant 2r \tag{6}$$

是一凸域. 今先求凸域 (6) 之面積

$$\iint\limits_{|\xi|+|\eta|\leqslant 2r} dx\,dy = \iint\limits_{|\xi|+|\eta|\leqslant 2r} \left| \frac{\partial(x, y)}{\partial(\xi, \eta)} \right| d\xi\,d\eta = \frac{1}{|\Delta|} \iint\limits_{|\xi|+|\eta|\leqslant 2r} d\xi\,d\eta = \frac{8r^2}{|\Delta|}.$$

即得:

定理 5. 必有一異於原點之整點使

$$|\xi| + |\eta| \leqslant (2|\Delta|)^{\frac{1}{2}}.$$

由 (5) 立得:

定理 6. 必有一異於原點之整點使

$$|\xi\eta| \leqslant \frac{1}{2}|\Delta|.$$

此定理也非最好之定理,已有人證明 $\frac{1}{2}$ 可代以 $\frac{1}{\sqrt{5}}$.

§ 2. Minkowski 之基本定理.

R 爲 n 維空間中的有限域,如 R 內任意二點聯線的中點恆在 R 內,則 R 稱爲凸域.

定理 1. 在 n 維空間中任一以原點爲對稱中心且體積大於 2^n 之凸域 R (或稱凸體),必包有一異於原點之整點.

定理 1.1 之證明不難推廣到 n 維空間. 今用另一方法證明本節之定理 1.

證: 命 t 爲一固定之正整數, q_r 跑過所有的整數. 則諸平面

$$x_r = \frac{2q_r}{t}, \qquad r = 1, 2, \cdots, n$$

分空間爲立方體,每一立方體之體積等於 $\left(\frac{2}{t}\right)^n$, 其角點爲 $\left(\frac{2q_1}{t}, \cdots, \frac{2q_n}{t}\right)$. 命 $N(t)$ 表示角點在 R 中之個數, A 表示 R 之體積,則由積分之定義可知

$$\lim_{t\to\infty}\left(\frac{2}{t}\right)^n N(t) = A.$$

若 $A > 2^n$, 則當 t 充分大時,卽有 $N(t) > t^n$.

另一方面, $(q_1, \cdots, q_n)$ 中最多祇有 t^n 組互不同餘, mod t, 卽 R 中必有二點

$$\left(\frac{2q_1}{t}, \cdots, \frac{2q_n}{t}\right), \left(\frac{2q_1'}{t}, \cdots, \frac{2q_n'}{t}\right)$$

適合 $q_i - q_i' \equiv 0 \pmod t$. 由於 R 以原點爲對稱中心,故 R 包有

$$\left(-\frac{2q_1'}{t}, \cdots, -\frac{2q_n'}{t}\right).$$

又由於 R 爲凸域,故 R 中亦包有

$$\left(\frac{2q_1}{t}, \cdots, \frac{2q_n}{t}\right) \text{ 及 } \left(-\frac{2q_1'}{t}, \cdots, -\frac{2q_n'}{t}\right)$$

之中點

$$\left(\frac{q_1-q_1'}{t},\cdots,\frac{q_n-q_n'}{t}\right).$$

此乃一整點．故得定理．

同理亦得：

定理 2. 若在定理 1 中，將條件“$>2^n$”改爲“$\geqslant 2^n$”；而將結果“在 R 中”改爲“在 R 中或邊界上”，則定理 1 依然成立．

更精密些有次之

定理 3. 由原點 O 作一射線交凸體 R 於 P．取 OP 之中點 Q，當 P 過凸體上之所有點，則 Q 描繪出一凸體，命之爲 $R_{\frac{1}{2}}$，在定理 2 之條件下，可假定得出之整點在 $R_{\frac{1}{2}}$ 之外．

證：命 ρ 爲由原點 O 到 R 邊上之最大距離．取一整數 N 使 $2^{N-1}\leqslant\rho<2^N$，則 $R_{2^{-N}}$ 之邊界點與原點之距離必小於 1．故 $R_{2^{-N}}$ 中除原點外無其他整點，故定理 2 中所得之整點必在 $R_{2^{-N}}$ 之外．故有一整數 m，在 $R_{2^{-m}}$ 中或其邊界上及 $R_{2^{-m-1}}$ 外有一整點 $(x_1,\cdots,x_n)$．因而整點

$$(2^m x_1,\cdots,2^m x_n)$$

在 R 中或其邊界上及 $R_{\frac{1}{2}}$ 之外．

§ 3. 一次線性式．

命 α_{rs} 爲實數，及

$$\xi_r=\alpha_{r1}x_1+\cdots+\alpha_{rn}x_n,\qquad r=1,2,\cdots,n. \tag{1}$$

行列式

$$\Delta=\begin{vmatrix}\alpha_{11}\cdots\alpha_{1n}\\ \cdots\cdots\cdots\cdots\\ \alpha_{n1}\cdots\alpha_{nn}\end{vmatrix}\neq 0.$$

取 R 爲

$$|\xi_1|\leqslant\lambda_1,\quad |\xi_2|\leqslant\lambda_2,\cdots,|\xi_n|\leqslant\lambda_n.$$

此爲一以原點爲對稱中心之凸體，其體積爲

$$\int\cdots\int_{|\xi_1|\leqslant\lambda_1,\cdots,|\xi_n|\leqslant\lambda_n} dx_1\cdot dx_2\cdots dx_n=\int\cdots\int_{|\xi_1|\leqslant\lambda_1,\cdots,|\xi_n|\leqslant\lambda_n}\left|\frac{\partial(x_1,x_2,\cdots,x_n)}{\partial(\xi_1,\xi_2,\cdots,\xi_n)}\right|d\xi_1\cdot d\xi_2\cdots d\xi_n=$$

$$= \frac{1}{|\Delta|} \int_{|\xi_1| \leqslant \lambda_1, \cdots, |\xi_n| \leqslant \lambda_n} \cdots \int d\xi_1 \cdot d\xi_2 \cdots d\xi_n = \frac{2^n \lambda_1 \lambda_2 \cdots \lambda_n}{|\Delta|}.$$

故若 $\lambda_1 \lambda_2 \cdots \lambda_n > |\Delta|$，則 R 中有一異於原點之整點. 若 $\lambda_1 \lambda_2 \cdots \lambda_n \geqslant |\Delta|$，則有一異於原點之整點在 R 內或在其邊界上. 故得:

定理 1. 若 $\xi_1, \cdots, \xi_n$ 是具實係數的 n 個變數 $x_1, \cdots, x_n$ 的線性式，其係數行列式是 Δ; $\lambda_1, \cdots, \lambda_n$ 是 n 個正數，且

$$\lambda_1 \lambda_2 \cdots \lambda_n \geqslant |\Delta|,$$

則有整數 $x_1, x_2, \cdots, x_n$ 非皆爲零，使

$$|\xi_1| \leqslant \lambda_1, \quad |\xi_2| \leqslant \lambda_2, \cdots, |\xi_n| \leqslant \lambda_n.$$

定理 2. 定理 1 之結論可以加強，卽有整數 $x_1, x_2, \cdots, x_n$ 非皆爲 0，使

$$|\xi_1| \leqslant \lambda_1, \quad |\xi_2| < \lambda_2, \cdots, |\xi_n| < \lambda_n.$$

證: 命 ε 爲一正數. 由定理 1 已知有非皆爲零之 $x_1, \cdots, x_n$，使

$$|\xi_1| \leqslant (1+\varepsilon)^{n-1} \lambda_1, \quad |\xi_2| \leqslant \frac{\lambda_2}{1+\varepsilon} < \lambda_2, \cdots, \quad |\xi_n| \leqslant \frac{\lambda_n}{1+\varepsilon} < \lambda_n.$$

當 $\varepsilon \to 0$ 時，由於整點的不連續性，故得定理.

取 $n+1$ 代替 n，取

$$\xi_\nu = x_\nu \ (1 \leqslant \nu \leqslant n), \ \xi_{n+1} = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n + x_{n+1},$$

$$\lambda_\nu = t^{1/n} \ (1 \leqslant \nu \leqslant n), \lambda_{n+1} = \frac{1}{t},$$

則由定理 2 可得:

定理 3. 必有一組整數 $x_1, \cdots, x_n$ 及 y，不全爲 0，使

$$|\alpha_1 x_1 + \cdots + \alpha_n x_n + y| < \frac{1}{t},$$

而

$$|x_\nu| \leqslant t^{1/n} \qquad (\text{此處 } t \text{ 爲任一實數} > 0),$$

又取

$$\xi_1 = x_{n+1}, \qquad \xi_{\nu+1} = x_\nu - \alpha_\nu x_{n+1} \qquad (1 \leqslant \nu \leqslant n),$$

$$\lambda_1 = t^n, \qquad \lambda_{\nu+1} = \frac{1}{t} \qquad (1 \leqslant \nu \leqslant n),$$

則得:

定理 4. 命 $\alpha_1, \cdots, \alpha_n$ 爲一組實數及 $t \geqslant 1$. 必有一異於原點之整點

$(x, y_1, y_2, \cdots, y_n)$ 使

$$|\alpha_\nu x - y_\nu| < \frac{1}{t}, \qquad 1 \leqslant x \leqslant t^n.$$

換言之,必有一組以 x 爲公分母之 n 個數 $\left(\frac{y_1}{x}, \cdots, \frac{y_n}{x}\right)$ 使

$$\left|\alpha_\nu - \frac{y_\nu}{x}\right| < \frac{1}{x^{1+1/n}}, \qquad 1 \leqslant \nu \leqslant n.$$

命 c_n 爲有以下性質之最大正實數: 若 $0 < c < c_n$, 則

$$\left|\alpha_\nu - \frac{y_\nu}{x}\right| < \frac{1}{cx^{1+1/n}}, \qquad 1 \leqslant \nu \leqslant n$$

有無窮組解. 由定理 10.4.4, 已知 $c_1 = \sqrt{5}$. 但當 $n \geqslant 2$ 時, 這問題還未解決.

定理 2 建議,是否連 $|\xi_1| \leqslant \lambda_1$ 也可改爲 $|\xi_1| < \lambda_1$, 此不可能. 例如:

$$\xi_1 = x_1, \quad \xi_2 = \alpha_{21} x_1 + x_2, \quad \xi_3 = \alpha_{31} x_1 + \alpha_{32} x_2 + x_3, \cdots,$$
$$\xi_n = \alpha_{n1} x_1 + \alpha_{n2} x_2 + \cdots + \alpha_{nn-1} x_{n-1} + x_n. \tag{2}$$

則由 $|\xi_1| < 1$, 可得 $x_1 = 0$; 再由 $|\xi_2| < 1$, 可得 $x_2 = 0$; 等等. 故僅有原點使

$$|\xi_1| < 1, \qquad |\xi_2| < 1, \quad \cdots, \qquad |\xi_n| < 1.$$

再命

$$x_\nu = \sum_{\mu=1}^{n} a_{\nu\mu} y_\mu \qquad (1 \leqslant \nu \leqslant n)$$

表一模變換. 將此代入 (2) 所得之齊次式也有與 (2) 同樣之性質. 問題: 除去所列舉之情況外,能否一起改爲 "$<$" 號. 此乃有名的 Minkowski 問題. 數十年來僅能證明 $n \leqslant 7$ 時之情況, 1942 年匈牙利數學家 Hajös 才一般地予以解決.

§4. 二次定正型.

今往研究橢球 R:

$$\xi_1^2 + \cdots + \xi_n^2 \leqslant r^2. \tag{1}$$

爲了證明 (1) 是凸體,祇須證明

$$\left(\frac{\xi_1+\xi_1'}{2}\right)^2 + \cdots + \left(\frac{\xi_n+\xi_n'}{2}\right)^2 \leqslant \frac{1}{2}\left\{(\xi_1^2 + \cdots + \xi_n^2) + (\xi_1'^2 + \cdots + \xi_n'^2)\right\}. \tag{2}$$

由於

$$\left(\frac{\xi_i+\xi_i'}{2}\right)^2 \leqslant \frac{\xi_i^2+\xi_i'^2}{2}, \qquad i=1,2,\cdots,n,$$

(2) 式顯然眞實.

因 n 維空間內半徑爲 r 的球體體積爲 $r^n\dfrac{\pi^{\frac{1}{2}n}}{\Gamma\left(\frac{1}{2}n+1\right)}$，故 R 之體積爲

$$\underset{\xi_1^2+\cdots+\xi_n^2\leqslant r^2}{\int\cdots\int} dx_1\cdots dx_n = \underset{\xi_1^2+\cdots+\xi_n^2\leqslant r^2}{\int\cdots\int}\left|\frac{\partial(x_1,\cdots,x_n)}{\partial(\xi_1,\cdots,\xi_n)}\right| d\xi_1\cdots d\xi_n =$$

$$=\frac{1}{|\Delta|}\underset{\xi_1^2+\cdots+\xi_n^2\leqslant r^2}{\int\cdots\int} d\xi_1\cdots d\xi_n = \frac{1}{|\Delta|} r^n \frac{\pi^{\frac{1}{2}n}}{\Gamma\left(\frac{1}{2}n+1\right)}.$$

於是得出:

定理 1. 有一組整數 $x_1,\cdots,x_n$ 不全爲 0，使

$$\xi_1^2+\cdots+\xi_n^2 \leqslant 4\left(\frac{|\Delta|}{J_n}\right)^{2/n},$$

此處

$$J_n = \frac{\pi^{\frac{1}{2}n}}{\Gamma\left(\frac{1}{2}n+1\right)}.$$

定理 1 可以換一種形式表示之. 二次定正型

$$Q(x_1,\cdots,x_n)=\sum_{r=1}^{n}\sum_{s=1}^{n} a_{rs}x_r x_s, \qquad a_{rs}=a_{sr}$$

可以表爲

$$Q=\xi_1^2+\cdots+\xi_n^2.$$

$\xi_1,\cdots,\xi_n$ 之行列式 Δ 之值爲 $D=|a_{rs}|$ 之值之平方根. 蓋因 $A=(a_{rs})$ 爲定正矩陣,故有矩陣 B 存在使 $A=BB'$, $\Delta=|B|=D^{\frac{1}{2}}$. 故定理 1 可以改述爲:

定理 2. 若 $Q(x_1,\cdots,x_n)$ 是一定正型,其行列式爲 D，則有一異於原點之整點 $x_1,\cdots,x_n$ 使

$$Q(x_1,\cdots,x_n)\leqslant 4\,J_n^{-2/n}\,D^{1/n}. \tag{3}$$

命 γ_n 是最小的常數有次之性質者: 有一異於原點之整點使

$$Q(x_1,\cdots,x_n)\leqslant \gamma_n D^{1/n}.$$

由 §1 已知 $\gamma_2=\frac{2}{\sqrt{3}}$. 迄今數學家僅知 $\gamma_n(2\leqslant n\leqslant 10)$ 之數值:

$$\gamma_3=\sqrt[3]{2},\quad \gamma_4=\sqrt{2},\quad \gamma_5=\sqrt[5]{8},\quad \gamma_6=\sqrt[6]{\frac{64}{3}},\quad \gamma_7=\sqrt[7]{64},\quad \gamma_8=2,$$

$$\gamma_9=2,\quad \gamma_{10}=2\sqrt[10]{\frac{4}{3}}.$$

一般言之,所知之結果為

$$\gamma_n<\frac{2}{\pi}\left(\Gamma\left(2+\frac{n}{2}\right)\right)^{2/n}\qquad\left(\sim\frac{n}{\pi e}\text{ 當 } n\to\infty\text{ 時}\right).$$

§5. 線性型之乘積.

先討論域 R:

$$|\xi_1|+\cdots+|\xi_n|\leqslant r. \tag{1}$$

此域顯然以原點為對稱中心,且由

$$\left|\frac{\xi+\xi'}{2}\right|\leqslant\frac{1}{2}\left(|\xi|+|\xi'|\right)$$

可知 R 是凸體,其體積等於

$$\int\limits_{|\xi_1|+\cdots+|\xi_n|\leqslant r}\!\!\cdots\!\!\int dx_1\cdots dx_n=\int\limits_{|\xi_1|+\cdots+|\xi_n|\leqslant r}\!\!\cdots\!\!\int\left|\frac{\partial(x_1,\cdots,x_n)}{\partial(\xi_1,\cdots,\xi_n)}\right|d\xi_1\cdots d\xi_n=$$

$$=\frac{1}{|\Delta|}\int\limits_{|\xi_1|+\cdots+|\xi_n|\leqslant r}\!\!\cdots\!\!\int d\xi_1\cdots d\xi_n=\frac{2^n}{|\Delta|}\int\limits_{\substack{\xi_1+\cdots+\xi_n\leqslant r\\ \xi_i\geqslant 0}}\!\!\cdots\!\!\int d\xi_1\cdots d\xi_n=\frac{2^n r^n}{n!|\Delta|}.$$

故得:

定理 1. 有一異於原點之整點 $(x_1,\cdots,x_n)$ 使

$$|\xi_1|+\cdots+|\xi_n|\leqslant(n!|\Delta|)^{1/n}. \tag{2}$$

當 $n=2$ 時,此乃最佳之結果. 蓋若取 $\xi_1=x+y$, $\xi_2=x-y$, 則 $|\Delta|=2$, 而 (2) 變為 $|\xi_1|+|\xi_2|\leqslant 2$. 但由於

$$|\xi_1|+|\xi_2|=\max(|\xi_1+\xi_2|,|\xi_1-\xi_2|)=2\max(|x|,|y|),$$

故若此小於 2, 則 $x=y=0$. 當 $n=3$ 時, Minkowski 曾證明有一異於原點之整點 (x_1,x_2,x_3) 使

$$|\xi_1|+|\xi_2|+|\xi_3|\leqslant\left(\frac{108}{19}|\Delta|\right)^{1/3},$$

且此處 $\frac{108}{19}$ 是最佳者. 當 $n>3$ 時,此乃一未解決之問題.

在今後討論線性型之乘積時，將用及下之

定理 2. 若 $a_1 \geqslant 0, \cdots, a_n \geqslant 0$，則

$$(a_1 \cdots a_n)^{1/n} \leqslant \frac{a_1+\cdots+a_n}{n}.$$

證: 1) $n=2^k$ 時，用歸納法. 已知當 $k=1$ 時有

$$(a_1 a_2)^{1/2} \leqslant \frac{a_1+a_2}{2}.$$

今假定當 $n=2^{k-1}$ 時，定理為真. 則當 $n=2^k$ 時有

$$(a_1 \cdots a_{2^k})^{\frac{1}{2^k}} = \left\{(a_1 \cdots a_{2^{k-1}})^{\frac{1}{2^{k-1}}} (a_{2^{k-1}+1} \cdots a_{2^k})^{\frac{1}{2^{k-1}}}\right\}^{1/2} \leqslant$$

$$\leqslant \left\{\left(\frac{a_1+\cdots+a_{2^{k-1}}}{2^{k-1}}\right)\left(\frac{a_{2^{k-1}+1}+\cdots+a_{2^k}}{2^{k-1}}\right)\right\}^{1/2} \leqslant$$

$$\leqslant \frac{a_1+\cdots+a_{2^k}}{2^k}.$$

2)（反向歸納法）今往證明若定理對 $n+1$ 為真，則對 n 為真. 取

$$a_{n+1} = \frac{1}{n}(a_1+\cdots+a_n).$$

由假定可知

$$\left(\frac{1}{n} a_1 \cdots a_n (a_1+\cdots+a_n)\right)^{\frac{1}{n+1}} = (a_1 \cdots a_{n+1})^{\frac{1}{n+1}} \leqslant \frac{a_1+\cdots+a_{n+1}}{n+1} =$$

$$= \frac{1}{n+1}\left\{a_1+\cdots+a_n+\frac{1}{n}(a_1+\cdots+a_n)\right\} =$$

$$= \frac{a_1+\cdots+a_n}{n},$$

故得

$$(a_1 \cdots a_n)^{\frac{1}{n+1}} \leqslant \left(\frac{a_1+\cdots+a_n}{n}\right)^{1-\frac{1}{n+1}} = \left(\frac{a_1+\cdots+a_n}{n}\right)^{\frac{n}{n+1}},$$

卽得定理.

由定理 1 及定理 2 立得:

定理 3. 有一異於原點之整點使

$$|\xi_1 \cdots \xi_n| \leqslant \frac{n!}{n^n} |\Delta|.$$

注意: 由 §3 之定理 1 亦可得出,必有一異於原點之整點使

$$|\xi_1\cdots\xi_n|\leqslant|\Delta|.$$

由於當 $n>1$ 時 $n!<n^n$, 故本節之定理 3 較佳. 命 γ_n 代表最小的正實數,使凡 $\gamma\geqslant\gamma_n$, 則必有一異於原點之整點使

$$|\xi_1\cdots\xi_n|\leqslant\gamma|\Delta|.$$

今僅知 $\gamma_2=\frac{1}{\sqrt{5}}$, $\gamma_3=\frac{1}{7}$ (Davenport). 定出 $\gamma_n\ (n\geqslant4)$ 爲一尙未解決之問題.

§6. **聯立漸近法.**

定理 1. 若 $\alpha_1,\cdots,\alpha_n$ 是 n 個實數,則有一異於原點之整點 $(x_1,\cdots,x_n)$ 及整數 $y(\geqslant1)$ 使

$$\left|\alpha_i-\frac{x_i}{y}\right|\leqslant\frac{n}{(n+1)y^{1+\frac{1}{n}}},\quad i=1,2,\cdots,n.$$

證: 先研究

$$|x_i-\alpha_i y|+\left|\frac{y}{t}\right|\leqslant r,\qquad 1\leqslant i\leqslant n,\qquad t\neq0.$$

此乃一以原點爲對稱中心之凸體,其體積等於

$$\underset{\substack{|\xi_i|+|\xi_{n+1}|\leqslant r\\ i=1,\cdots,n}}{\int\cdots\int} dx_1\cdots dx_n\,dy\qquad\left(\begin{array}{r}\text{此處 }\xi_i=x_i-\alpha_i y,\quad 1\leqslant i\leqslant n,\\ \xi_{n+1}=\dfrac{y}{t}.\end{array}\right)=$$

$$=\underset{\substack{|\xi_i|+|\xi_{n+1}|\leqslant r\\ i=1,\cdots,n}}{\int\cdots\int}\left|\frac{\partial(x_1,\cdots,x_n,y)}{\partial(\xi_1,\cdots,\xi_n,\xi_{n+1})}\right|d\xi_1\cdots d\xi_n\,d\xi_{n+1}=$$

$$=|t|\underset{\substack{|\xi_i|+|\xi_{n+1}|\leqslant r\\ i=1,\cdots,n}}{\int\cdots\int}d\xi_1\cdots d\xi_n\,d\xi_{n+1}=2^{n+1}|t|\underset{\substack{\xi_i+\xi_{n+1}\leqslant r\\ i=1,\cdots,n\\ \xi_i\geqslant0,\ \xi_{n+1}\geqslant0}}{\int\cdots\int}d\xi_1\cdots d\xi_n\,d\xi_{n+1}=$$

$$=\frac{2^{n+1}|t|}{n+1}r^{n+1}.$$

於是卽有一異於原點之整點 $(x_1,\cdots,x_n,y)$ 使

$$|x_i-\alpha_i y|+\left|\frac{y}{t}\right|\leqslant\left(\frac{n+1}{|t|}\right)^{\frac{1}{n+1}}.$$

由定理 5.2 可知

$$\left|(x_i-\alpha_i y)^n\left(\frac{ny}{t}\right)\right|^{\frac{1}{n+1}} \leqslant \frac{n|x_i-\alpha_i y|+n\left|\frac{y}{t}\right|}{n+1} \leqslant \frac{n}{n+1}\left(\frac{n+1}{|t|}\right)^{\frac{1}{n+1}}, \quad i=1,\cdots,n.$$

卽得

$$\left|\alpha_i-\frac{x_i}{y}\right| \leqslant \frac{n}{(n+1)y^{1+\frac{1}{n}}}, \qquad i=1,2,\cdots,n.$$

此定理略佳於定理 3.4. 迄今最佳之結果爲

$$c_n \geqslant \gamma_n, \qquad \gamma_n=\frac{n+1}{n}\left\{1+\left(\frac{n-1}{n+1}\right)^{n+3}\right\}^{1/n}$$

(Blichfeldt). $\left(c_3 \geqslant \sqrt{\frac{19}{8}},\right.$ Minkowski.$\left.\right)$

習題. 若 $\alpha_v=\beta_v+i\gamma_v$ $(v=1,\cdots,n)$ 是 n 個複數, 則有複整數 $z_1,\cdots,z_n, w$ 存在,使

$$\left|\alpha_v-\frac{z_v}{w}\right| \leqslant \frac{n}{n+1}\cdot\frac{2}{\sqrt{\pi}}\left(\frac{2n+1}{n+1}\cdot\frac{4}{\pi}\right)^{\frac{1}{2n}}\frac{1}{|w|^{1+\frac{1}{n}}}.$$

§ 7. Minkowski 不等式.

當 $a_i \geqslant 0$ $(i=1,\cdots,n)$, $r>0$ 時,定義

$$M_r(a)=\left\{\frac{1}{n}(a_1^r+\cdots+a_n^r)\right\}^{1/r}. \tag{1}$$

當 $r<0$ 且某一 $a_i=0$ 時, (1) 式無意義. 此時定義 $(a_1^r+\cdots+a_n^r)^{\frac{1}{r}}=0$. 於是當 $a_i \geqslant 0$, $r \neq 0$ 時,均可定義

$$M_r(a)=\left\{\frac{1}{n}(a_1^r+\cdots+a_n^r)\right\}^{1/r}.$$

但 $r<0$ 且某一 $a_i=0$ 時, $M_r(a)=0$. 今後將 $a_i \geqslant 0$ $(i=1,\cdots,n)$ 記爲 (a). $(a)>0$ 表示 $a_i>0$ $(i=1,\cdots,n)$. $(a)\neq 0$ 表示 a_i 不全爲零. $a_i \geqslant 0 (i=1,\cdots,n)$ 中之最大者記爲 $\max a$, 最小者記爲 $\min a$.

如有不全爲 0 之實數 λ, μ, 使 $\lambda a_i=\mu b_i$ $(i=1,\cdots,n)$, 則稱 (a) 與 (b) 成比例.

定理 1. $\lim\limits_{r\to+\infty} M_r(a)=\max a$.

證: 因 $r\to+\infty$, 可設 $r>0$. 於是有

$$\left\{\frac{1}{n}(\max a)^r\right\}^{1/r}\leqslant M_r(a)\leqslant\left\{(\max a)^r\right\}^{1/r},$$

即

$$\left(\frac{1}{n}\right)^{1/r}\max a\leqslant M_r(a)\leqslant\max a.$$

因 $\lim\limits_{r\to+\infty}\left(\frac{1}{n}\right)^{1/r}=\left(\frac{1}{n}\right)^0=1$, 故得 $\lim\limits_{r\to+\infty}M_r(a)=\max a$.

定理 2. $\lim\limits_{r\to-\infty}M_r(a)=\min a$.

證: 因 $r\to-\infty$, 可設 $r<0$. $(a)>0$ 時,

$$M_r(a)=\left\{\frac{1}{n}(a_1^r+\cdots+a_n^r)\right\}^{1/r}=\frac{1}{\left\{\frac{1}{n}\left[\left(\frac{1}{a_1}\right)^{-r}+\cdots+\left(\frac{1}{a_n}\right)^{-r}\right]\right\}^{1/-r}}=$$

$$=\frac{1}{M_{-r}\left(\frac{1}{a}\right)}.$$

於是由定理 1,

$$\lim_{r\to-\infty}M_r(a)=\frac{1}{\lim\limits_{-r\to+\infty}M_{-r}\left(\frac{1}{a}\right)}=\frac{1}{\max\frac{1}{a}}=\min a.$$

當 $r<0$ 且某一 $a_i=0$ 時, $M_r(a)$ 及 $\min a$ 均爲 0. 仍有

$$\lim_{r\to-\infty}M_r(a)=\min a.$$

定理證完.

定理 3. $\lim\limits_{r\to0}M_r(a)=(a_1\cdots a_n)^{\frac{1}{n}}$, $(a_1\cdots a_n)^{\frac{1}{n}}$ 卽普通 n 個實數 $(\geqslant0)$ 之幾何平均值,記爲 $G(a)$.

證: 1) $r<0$, 且某一 $a_i=0$, 則定理顯然成立.

2) $r\neq0$, $(a)>0$ 時,由 (1) 有

$$M_r(a)=\left\{\frac{1}{n}(a_1^r+\cdots+a_n^r)\right\}^{1/r}=$$

$$=e^{\frac{1}{r}\log\left\{\frac{1}{n}(a_1^r+\cdots+a_n^r)\right\}}.$$

當 $r\to0$ 時,利用求極限的 L'Hospital 法則,可知

$$\lim_{r\to0}\frac{1}{r}\log\left\{\frac{1}{n}(a_1^r+\cdots+a_n^r)\right\}=$$

$$= \lim_{r\to 0} \frac{\frac{1}{n}\sum_{i=1}^{n} a_i^r \log a_i}{\frac{1}{n}(a_1^r+\cdots+a_n^r)} = \frac{1}{n}\sum_{i=1}^{n} \log a_i .$$

於是

$$\lim_{r\to 0} M_r(a) = \lim_{r\to 0} e^{\frac{1}{r}\log\left\{\frac{1}{n}(a_1^r+\cdots+a_n^r)\right\}} =$$

$$= e^{\frac{1}{n}\sum_{i=1}^{n}\log a_i} = e^{\log(a_1\cdots a_n)^{1/n}} = (a_1\cdots a_n)^{1/n} = G(a) .$$

3) $r>0$，且 a_i 中有某些個爲 0，則不妨假定 $a_1>0, \cdots, a_s>0$, $a_{s+1}=a_{s+2}=\cdots=a_n=0$， $s<n$． 於是有

$$M_r(a) = \left\{\frac{1}{n}(a_1^r+\cdots+a_s^r)\right\}^{1/r} = \left\{\frac{s}{n}\cdot\frac{1}{s}(a_1^r+\cdots+a_s^r)\right\}^{1/r} =$$

$$= \left(\frac{s}{n}\right)^{1/r}\left\{\frac{1}{s}(a_1^r+\cdots+a_s^r)\right\}^{1/r} .$$

由前之結果,有 $\lim_{r\to 0}\left\{\frac{1}{s}(a_1^r+\cdots+a_s^r)\right\}^{1/r} = (a_1\cdots a_s)^{1/s}$． 又 $\frac{s}{n}<1$，當 $r\to 0$ 時,

$$\lim_{r\to 0}\left(\frac{s}{n}\right)^{1/r} = 0 .$$

所以當 $r>0$，某些 $a_i=0$ 時,仍有

$$\lim_{r\to 0} M_r(a) = \lim_{r\to 0}\left\{\left(\frac{s}{n}\right)^{1/r}\left\{\frac{1}{s}(a_1^r+\cdots+a_s^r)\right\}^{1/r}\right\} = 0\cdot(a_1\cdots a_s)^{1/s} = 0 =$$

$$= (a_1\cdots a_n)^{1/n} .$$

定理證完.

引 1. 若 $\alpha+\beta=1$，$\alpha>0$，$\beta>0$，則對 $s\geqslant 0$，$t\geqslant 0$，恆有

$$s^{\alpha} t^{\beta} \leqslant s\alpha + t\beta ,$$

且等號只當 $s=t$ 時成立.

證: 當 $s=t$ 或 s, t 中之一爲 0 時，引 1 之前半部分顯然成立． 今往證明 s, t 均 >0 且 $s\neq t$ 時之情形.

設 $s>t$，則 $\frac{s}{t}>1$． 又 $0<\alpha<1$，$1-\alpha=\beta$，故有

$$\left(\frac{s}{t}\right)^{\alpha}-1=\alpha\int_{1}^{s/t} y^{\alpha-1}\,dy \leqslant \alpha\int_{1}^{s/t} dy=\alpha\left(\frac{s}{t}-1\right).$$

由

$$\left(\frac{s}{t}\right)^{\alpha}-1 \leqslant \alpha\left(\frac{s}{t}-1\right),$$

立得

$$s^{\alpha} t^{\beta} \leqslant s\alpha + t\beta.$$

若 $s^{\alpha} t^{\beta}=s\alpha+t\beta$, 而 $s \neq t$, 因為 s, t 對稱的關係,不妨假定 $s>t$. 於是有

$$\alpha\int_{1}^{s/t} y^{\alpha-1}\,dy=\alpha\int_{1}^{s/t} dy,$$

亦即

$$\int_{1}^{s/t}\left(y^{\alpha-1}-1\right) dy=0.$$

此為不可能之事,所以必須 $s=t$.

引 2 (Hölder 不等式). 若 $\alpha+\beta=1$, $\alpha>0$, $\beta>0$. 則當 (a) 與 (b) 不成比例時,恆有

$$\sum_{i=1}^{n} a_i^{\alpha} b_i^{\beta}<\left(\sum_{i=1}^{n} a_i\right)^{\alpha}\left(\sum_{i=1}^{n} b_i\right)^{\beta}.$$

證: 因 (a) 與 (b) 不成比例,故必有 i 存在 $(1 \leqslant i \leqslant n)$ 使

$$\frac{a_i}{\sum_{j=1}^{n} a_j} \neq \frac{b_i}{\sum_{j=1}^{n} b_j}.$$

於是由引 1,

$$\frac{\sum_{i=1}^{n} a_i^{\alpha} b_i^{\beta}}{\left(\sum_{j=1}^{n} a_j\right)^{\alpha}\left(\sum_{j=1}^{n} b_j\right)^{\beta}}=\sum_{i=1}^{n}\left(\frac{a_i}{\sum_{j=1}^{n} a_j}\right)^{\alpha}\left(\frac{b_i}{\sum_{j=1}^{n} b_j}\right)^{\beta}<$$

$$<\sum_{i=1}^{n}\left\{\left(\frac{a_i}{\sum_{j=1}^{n} a_j}\right)\alpha+\left(\frac{b_i}{\sum_{j=1}^{n} b_j}\right)\beta\right\}=\alpha+\beta=1$$

故得

$$\sum_{i=1}^{n} a_i^{\alpha} b_i^{\beta} < \left(\sum_{i=1}^{n} a_i\right)^{\alpha} \left(\sum_{i=1}^{n} b_i\right)^{\beta}.$$

引 3 (Hölder 不等式). 若 $k>0$, $k\neq 1$, $\frac{1}{k}+\frac{1}{k'}=1$, 則當 (a^k), $(b^{k'})$ 不成比例且 $(ab)\neq 0$ 時,恆有

$$\sum_{i=1}^{n} a_i b_i < \left(\sum_{i=1}^{n} a_i^k\right)^{1/k} \left(\sum_{i=1}^{n} b_i^{k'}\right)^{1/k'} \qquad (k>1), \tag{2}$$

$$\sum_{i=1}^{n} a_i b_i > \left(\sum_{i=1}^{n} a_i^k\right)^{1/k} \left(\sum_{i=1}^{n} b_i^{k'}\right)^{1/k'} \qquad (k<1). \tag{3}$$

證: 1) $k>1$ 的情形. 此時 $k'=\frac{k}{k-1}>1$, $0<\frac{1}{k}<1$, $0<\frac{1}{k'}<1$, $\frac{1}{k}+\frac{1}{k'}=1$. 由引 2, 有

$$\sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} (a_i^k)^{1/k} (b_i^{k'})^{1/k'} < \left(\sum_{i=1}^{n} a_i^k\right)^{1/k} \left(\sum_{i=1}^{n} b_i^{k'}\right)^{1/k'}.$$

2) $0<k<1$ 的情形. 此時 $k'=\frac{k}{k-1}<0$. 若某些 $b_i=0$, 則由本節開始時之定義可知 $\left(\sum_{i=1}^{n} b_i^{k'}\right)^{1/k'}=0$. 於是

$$\sum_{i=1}^{n} a_i b_i > 0 = \left(\sum_{i=1}^{n} a_i^k\right)^{1/k} \left(\sum_{i=1}^{n} b_i^{k'}\right)^{1/k'}.$$

當 $(b)>0$ 時,由 $0<k<1$, 可知

$$0<\frac{1}{\left(\frac{1}{k}\right)}<1,\ 0<\frac{1}{\left(-\frac{k'}{k}\right)}=1-k<1,\ \frac{1}{\left(\frac{1}{k}\right)}+\frac{1}{\left(-\frac{k'}{k}\right)}=1.$$

由引 2 可得

$$\sum_{i=1}^{n} a_i^k = \sum_{i=1}^{n} (a_i b_i)^k b_i^{-k} = \sum_{i=1}^{n} (a_i b_i)^{\frac{1}{\left(\frac{1}{k}\right)}} (b_i^{k'})^{\frac{1}{\left(-\frac{k'}{k}\right)}} <$$

$$< \left(\sum_{i=1}^{n} a_i b_i\right)^{\frac{1}{\left(\frac{1}{k}\right)}} \left(\sum_{i=1}^{n} b_i^{k'}\right)^{\frac{1}{\left(-\frac{k'}{k}\right)}} =$$

$$=\left(\sum_{i=1}^{n} a_i\ b_i\right)^k\left(\sum_{i=1}^{n} b_i^{k'}\right)^{-\frac{k}{k'}}.$$

由

$$\sum_{i=1}^{n} a_i^k<\left(\sum_{i=1}^{n} a_i b_i\right)^k\left(\sum_{i=1}^{n} b_i^{k'}\right)^{-\frac{k}{k'}},$$

立得

$$\sum_{i=1}^{n} a_i b_i>\left(\sum_{i=1}^{n} a_i^k\right)^{\frac{1}{k}}\left(\sum_{i=1}^{n} b_i^{k'}\right)^{\frac{1}{k'}} \qquad (k<1).$$

定理 4. $0<r<s$，除去 $a_1=a_2=\cdots=a_n$ 的情形外，恆有

$$M_r(a)<M_s(a).$$

證： 令 $r=s\alpha$，$0<\alpha<1$. 則有

$$M_r(a)=\left\{\frac{1}{n}(a_1^r+\cdots+a_n^r)\right\}^{1/r}=\left\{\frac{1}{n}(a_1^{s\alpha}+\cdots+a_n^{s\alpha})\right\}^{1/s\alpha}=$$

$$=\left(\frac{1}{n}\left\{\sum_{i=1}^{n}(a_i^s)^\alpha\cdot 1\right\}\right)^{1/s\alpha}.$$

由引 2，得

$$M_r(a)=\left(\frac{1}{n}\left\{\sum_{i=1}^{n}(a_i^s)^\alpha\cdot 1^{1-\alpha}\right\}\right)^{1/s\alpha}<\left\{\frac{1}{n}\left(\sum_{i=1}^{n} a_i^s\right)^\alpha\left(\sum_{i=1}^{n} 1\right)^{1-\alpha}\right\}^{1/s\alpha}=$$

$$=\left\{\frac{1}{n}\left(\sum_{i=1}^{n} a_i^s\right)^\alpha n^{1-\alpha}\right\}^{1/s\alpha}=$$

$$=\left(\frac{(a_1^s+\cdots+a_n^s)^\alpha}{n^\alpha}\right)^{1/s\alpha}=$$

$$=\left(\frac{a_1^s+\cdot+a_n^s}{n}\right)^{1/s}=$$

$$=M_s(a).$$

定理證完.

定理 5. 若 (a) 與 (b) 不成比例，$r>0$，$r\neq 1$，則有

$$\left\{\sum_{i=1}^{n}(a_i+b_i)^r\right\}^{1/r}<\left(\sum_{i=1}^{n} a_i^r\right)^{1/r}+\left(\sum_{i=1}^{n} b_i^r\right)^{1/r} \qquad (r>1)$$

及

$$\left\{\sum_{i=1}^{n}(a_i+b_i)^r\right\}^{1/r}>\left(\sum_{i=1}^{n} a_i^r\right)^{1/r}+\left(\sum_{i=1}^{n} b_i^r\right)^{1/r} \qquad (r<1).$$

證: 1) $r>1$ 的情形.

令 $r'=\frac{r}{r-1}$, 則 $r'>1$, $\frac{1}{r}+\frac{1}{r'}=1$. 由引 3 之 (2) 式,有

$$\sum_{i=1}^{n}(a_i+b_i)^r=\sum_{i=1}^{n}a_i(a_i+b_i)^{r-1}+\sum_{i=1}^{n}b_i(a_i+b_i)^{r-1}<$$

$$<\left(\sum_{i=1}^{n}a_i^r\right)^{1/r}\left\{\sum_{i=1}^{n}((a_i+b_i)^{r-1})^{r'}\right\}^{1/r'}+$$

$$+\left(\sum_{i=1}^{n}b_i^r\right)^{1/r}\left\{\sum_{i=1}^{n}((a_i+b_i)^{r-1})^{r'}\right\}^{1/r'}=$$

$$=\left(\sum_{i=1}^{n}a_i^r\right)^{1/r}\left\{\sum_{i=1}^{n}(a_i+b_i)^r\right\}^{\frac{r-1}{r}}+\left(\sum_{i=1}^{n}b_i^r\right)^{1/r}\left\{\sum_{i=1}^{n}(a_i+b_i)^r\right\}^{\frac{r-1}{r}}=$$

$$=\left\{\left(\sum_{i=1}^{n}a_i^r\right)^{1/r}+\left(\sum_{i=1}^{n}b_i^r\right)^{1/r}\right\}\left\{\sum_{i=1}^{n}(a_i+b_i)^r\right\}^{\frac{r-1}{r}}.$$

兩端乘以 $\left\{\sum_{i=1}^{n}(a_i+b_i)^r\right\}^{-\frac{r-1}{r}}$, 則得

$$\left\{\sum_{i=1}^{n}(a_i+b_i)^r\right\}^{1/r}<\left(\sum_{i=1}^{n}a_i^r\right)^{1/r}+\left(\sum_{i=1}^{n}b_i^r\right)^{1/r}.$$

2) $0<r<1$ 的情形.

此時,恆有 i 存在, $1\leqslant i\leqslant n$, 使 $a_i+b_i>0$. 否則,若

$$a_i+b_i=0 \qquad (i=1,\cdots,n),$$

則由 $a_i\geqslant 0$, $b_i\geqslant 0$, 可知

$$a_i=b_i=0 \qquad (i=1,\cdots,n),$$

即 $(a)=(b)=0$. 此時 (a) 與 (b) 成比例,不在考慮之內.

不失一般性,可以假定 $a_i+b_i>0 \quad (i=1,\cdots,n)$.

此時, $0<r<1$, 令 $r'=\frac{r}{r-1}$, 則由引 3 之 (3) 式,有

$$\sum_{i=1}^{n}(a_i+b_i)^r=\sum_{i=1}^{n}a_i(a_i+b_i)^{r-1}+\sum_{i=1}^{n}b_i(a_i+b_i)^{r-1}>$$

$$>\left(\sum_{i=1}^{n} a_i^r\right)^{1/r}\left\{\sum_{i=1}^{n}((a_i+b_i)^{r-1})^{r'}\right\}^{1/r'}+$$

$$+\left(\sum_{i=1}^{n} b_i^r\right)^{1/r}\left\{\sum_{i=1}^{n}((a_i+b_i)^{r-1})^{r'}\right\}^{1/r'}=$$

$$=\left(\sum_{i=1}^{n} a_i^r\right)^{1/r}\left\{\sum_{i=1}^{n}(a_i+b_i)^r\right\}^{\frac{r-1}{r}}+\left(\sum_{i=1}^{n} b_i^r\right)^{1/r}\left\{\sum_{i=1}^{n}(a_i+b_i)^r\right\}^{\frac{r-1}{r}}=$$

$$=\left\{\left(\sum_{i=1}^{n} a_i^r\right)^{1/r}+\left(\sum_{i=1}^{n} b_i^r\right)^{1/r}\right\}\left\{\sum_{i=1}^{n}(a_i+b_i)^r\right\}^{\frac{r-1}{r}}.$$

兩端乘以 $\left\{\sum_{i=1}^{n}(a_i+b_i)^r\right\}^{-\frac{r-1}{r}}$， 則得

$$\left\{\sum_{i=1}^{n}(a_i+b_i)^r\right\}^{1/r}>\left(\sum_{i=1}^{n} a_i^r\right)^{1/r}+\left(\sum_{i=1}^{n} b_i^r\right)^{1/r}.$$

定理證完. 此定理卽通常所謂之 Minkowski 不等式.

§8. 線性型之乘方平均值.

定理 1. 命 $n\geqslant 2$. $\xi_1,\cdots,\xi_n$ 是 $x_1,\cdots,x_n$ 的 n 個線性型, 其行列式 $\Delta\neq 0$. 其中有 s 對型是有共軛複數係數的,有 r 個型是實係數的, $r+2s=n$ 若 $\sigma\geqslant 1$, 則有一異於原點之整點使

$$\left(\frac{|\xi_1|^\sigma+\cdots+|\xi_n|^\sigma}{n}\right)^{1/\sigma}\leqslant\left(\frac{\left(\frac{2}{\pi}\right)^s n^{-\frac{n}{\sigma}}\Gamma\left(1+\frac{n}{\sigma}\right)|\Delta|}{2^{-\frac{2s}{\sigma}}\Gamma^r\left(1+\frac{1}{\sigma}\right)\Gamma^s\left(1+\frac{2}{\sigma}\right)}\right)^{1/n}.$$

證: 由定理 7.5 已知

$$\left(\frac{|\xi_1|^\sigma+\cdots+|\xi_n|^\sigma}{n}\right)^{1/\sigma}\leqslant T \tag{1}$$

是一以原點爲對稱中心的凸體. 今往算出積分

$$A=\int\cdots\int_{|\xi_1|^\sigma+\cdots+|\xi_n|^\sigma\leqslant nT^\sigma} dx_1\cdots dx_n$$

之值.

命 $\xi_{r+j}=\eta_{r+j}+i\,\eta_{r+s+j}$, $\xi_{r+s+j}=\bar{\xi}_{r+j}$ $(j=1,2,\cdots,s)$ 是有共軛複數係數的 s 對線性型。如此則

$$A=\int\cdots\int_{|\xi_1|^\sigma+\cdots+|\xi_r|^\sigma+2\sum_{j=r+1}^{r+s}(\eta_j^2+\eta_{s+j}^2)^{\sigma/2}\leqslant nT^\sigma}\left|\frac{\partial(x_1,\cdots,x_n)}{\partial(\xi_1,\cdots,\xi_r,\eta_{r+1},\cdots,\eta_{r+2s})}\right|d\xi_1\cdots d\xi_r\,d\eta_{r+1}\cdots d\eta_{r+2s}=$$

$$=\frac{2^s}{|\Delta|}\int\cdots\int_{|\xi_1|^\sigma+\cdots+|\xi_r|^\sigma+2\sum_{j=r+1}^{r+s}(\eta_j^2+\eta_{s+j}^2)^{\sigma/2}\leqslant nT^\sigma}d\xi_1\cdots d\xi_r\,d\eta_{r+1}\cdots d\eta_{r+2s}.$$

換變數，令

$$\xi_1=\rho_1,\cdots,\xi_r=\rho_r,$$

$$\eta_{r+j}=\left(\frac{1}{2}\right)^{1/\sigma}\rho_{r+j}\cos\theta_{r+j},\quad \eta_{r+s+j}=\left(\frac{1}{2}\right)^{1/\sigma}\rho_{r+j}\sin\theta_{r+j},\quad 1\leqslant j\leqslant s.$$

如此，得

$$A=\frac{2^s\cdot 2^r\left(\frac{1}{2}\right)^{2s/\sigma}}{|\Delta|}\int\cdots\int_{\substack{\rho_1^\sigma+\cdots+\rho_{r+s}^\sigma\leqslant nT^\sigma\\ \rho_\nu\geqslant 0}}\left(\prod_{\nu=r+1}^{r+s}\rho_\nu\right)d\rho_1\cdots d\rho_{r+s}\int_0^{2\pi}\cdots\int_0^{2\pi}d\theta_{r+1}\cdots d\theta_{r+s}=$$

$$=\frac{2^{n-\frac{2s}{\sigma}}\pi^s}{|\Delta|}\int\cdots\int_{\substack{\rho_1^\sigma+\cdots+\rho_{r+s}^\sigma\leqslant nT^\sigma\\ \rho_\nu\geqslant 0}}\left(\prod_{\nu=r+1}^{r+s}\rho_\nu\right)d\rho_1\cdots d\rho_{r+s}.$$

命 $\rho_\nu^\sigma=n\,T^\sigma\tau_\nu$, $\nu=1,2,\cdots,r+s$, 則得

$$A=\frac{2^{n-\frac{2s}{\sigma}}\pi^s}{|\Delta|}(n^{1/\sigma}T)^n\left(\frac{1}{\sigma}\right)^{r+s}\int\cdots\int_{\substack{\tau_1+\cdots+\tau_{r+s}\leqslant 1\\ \tau_\nu\geqslant 0}}\tau_1^{\frac{1}{\sigma}-1}\cdots\tau_r^{\frac{1}{\sigma}-1}\tau_{r+1}^{\frac{2}{\sigma}-1}\cdots\tau_{r+s}^{\frac{2}{\sigma}-1}d\tau_1\cdots d\tau_{r+s}=$$

$$=\frac{1}{|\Delta|}2^{n-\frac{2s}{\sigma}}\pi^s(n^{1/\sigma}T)^n\left(\frac{1}{\sigma}\right)^{r+s}\frac{\Gamma^r\left(\frac{1}{\sigma}\right)\Gamma^s\left(\frac{2}{\sigma}\right)}{\Gamma\left(1+\frac{n}{\sigma}\right)}=$$

$$= (n^{1/\sigma} T)^n \, 2^{n-\frac{2s}{\sigma}} \left(\frac{\pi}{2}\right)^s \frac{\Gamma^r\left(1+\frac{1}{\sigma}\right)\Gamma^s\left(1+\frac{2}{\sigma}\right)}{|\Delta|\,\Gamma\left(1+\frac{n}{\sigma}\right)}.$$

當

$$A \geqslant 2^n$$

時,即

$$T \geqslant \left(\frac{\left(\frac{2}{\pi}\right)^s n^{-\frac{n}{\sigma}} \Gamma\left(1+\frac{n}{\sigma}\right)|\Delta|}{2^{-\frac{2s}{\sigma}} \Gamma^r\left(1+\frac{1}{\sigma}\right)\Gamma^s\left(1+\frac{2}{\sigma}\right)} \right)^{1/n}$$

時,有一異於原點之整點適合 (1) 式. 故得定理.

定理 2. 與定理 1 之假定同. 若 $\lambda_1, \cdots, \lambda_n$ 是 n 個正數, $\lambda_{r+t} = \lambda_{r+s+t}$ $(t = 1, \cdots, s)$ 及 $\lambda_1 \cdots \lambda_{r+2s} \geqslant \left(\frac{2}{\pi}\right)^s |\Delta|$, 則必有一異於原點之整點,使

$$|\xi_1| \leqslant \lambda_1, \cdots, |\xi_n| \leqslant \lambda_n.$$

讀者自證之.

定理 3. 與定理 1 之假定同. 命

$$\xi_\nu = \eta_\nu \quad (1 \leqslant \nu \leqslant r), \quad \xi_{r+\nu} = \eta_{r+\nu} + i\,\eta_{r+s+\nu}, \quad \xi_{r+s+\nu} = \bar{\xi}_{r+\nu} \quad (1 \leqslant \nu \leqslant s).$$

若 $\lambda_1 \cdots \lambda_n \geqslant \frac{|\Delta|}{2^s}$, 則有一異於原點之整點,使

$$|\eta_\nu| \leqslant \lambda_\nu, \quad 1 \leqslant \nu \leqslant n.$$

證: $\eta_1, \cdots, \eta_n$ 之行列式之絕對值等於 $\frac{|\Delta|}{2^s}$ 故可由定理 3.1 直接得之.

§ 9. Чеботарев 定理.

命

$$\xi_i = \sum_{j=1}^n a_{ij} x_j \qquad (i = 1, \cdots, n),$$

a_{ij} 爲實數,且係數行列式

$$\Delta = \begin{vmatrix} a_{11} \cdots a_{1n} \\ \cdots\cdots\cdots\cdots \\ a_{n1} \cdots a_{nn} \end{vmatrix} \neq 0.$$

著名之 Minkowski 猜測爲：對於任意一組實數 $\rho_1, \cdots, \rho_n$，恆有一組整數 $x_1, \cdots, x_n$ (可均爲 0) 使

$$|(\xi_1 - \rho_1) \cdots (\xi_n - \rho_n)| \leqslant \frac{1}{2^n} |\Delta|.$$

$n = 2$ 之情形已由 Minkowski 自己證明；$n = 3,4$ 之情形亦已有人證明；至於一般之情形，則有下列之定理.

定理 1 (Чеботарев). 命 m 爲 $|(\xi_1-\rho_1) \cdots (\xi_n-\rho_n)|$ 之下界，則

$$m \leqslant 2^{-\frac{n}{2}} |\Delta|.$$

證：不失其普遍性，可設 $\Delta = 1$, $m > 0$. 於是對任一 $\varepsilon > 0$，必有一組整數 $x_1^*, \cdots, x_n^*$ 使

$$\prod_{i=1}^{n} |\xi_i^* - \rho_i| = |(\xi_1^* - \rho_1) \cdots (\xi_n^* - \rho_n)| = \frac{m}{1-\theta}, \quad 0 \leqslant \theta < \varepsilon.$$

命

$$\xi_i' = \frac{\xi_i - \xi_i^*}{\xi_i^* - \rho_i} \qquad (i = 1, \cdots, n),$$

則

$$\xi_i' = \sum_{j=1}^{n} \beta_{ij}(x_j - x_j^*) \qquad (i = 1, \cdots, n),$$

且其係數行列式 D 之絕對值

$$|D| = \left(\prod_{i=1}^{n} |\xi_i^* - \rho_i|\right)^{-1} = \frac{1-\theta}{m}.$$

因 $\prod_{i=1}^{n} |\xi_i - \rho_i| \geqslant m$，故

$$\prod_{i=1}^{n} |\xi_i' + 1| = \prod_{i=1}^{n} \left|\frac{\xi_i - \rho_i}{\xi_i^* - \rho_i}\right| \geqslant 1 - \theta.$$

同理

$$\prod_{i=1}^{n} |\xi_i' - 1| \geqslant 1 - \theta.$$

於是

$$\prod_{i=1}^{n} |\xi_i'^2 - 1| \geqslant (1 - \theta)^2.$$

定義凸域 C'：

$$|\xi_i'| < \sqrt{1+(1-\theta)^2} \qquad (i=1,\cdots,n).$$

今往證明，C' 中除原點外，無整點。

若 C' 中有不同於原點的整點，則與之對應的 $\xi_1',\cdots,\xi_n'$ 必適合於

$$-1 \leqslant \xi_i'^2 - 1 < (1-\theta)^2 \leqslant 1, \quad |\xi_i'^2 - 1| \leqslant 1 \quad (i=1,\cdots,n);$$

若有 i 使 $\xi_i'^2 - 1 > -(1-\theta)^2$，則對此 i 有 $|\xi_i'^2 - 1| < (1-\theta)^2$，因之

$$\prod_{i=1}^{n} |\xi_i'^2 - 1| < (1-\theta)^2.$$

此不可能．故

$$-1 \leqslant \xi_i'^2 - 1 \leqslant -(1-\theta)^2 \qquad (i=1,\cdots,n).$$

因此

$$|\xi_i'| \leqslant \sqrt{1-(1-\theta)^2} \leqslant \sqrt{2\theta} \qquad (i=1,\cdots,n).$$

故知當 θ 很小時，若 C' 中有整點，則此整點必與原點十分接近；由此立可得出矛盾．蓋由定理 2.3，若 C' 中有異於原點之整點，則必有整點在 $C'_{\frac{1}{2}}$ 之外，此顯然與 $|\xi_i'| \leqslant \sqrt{2\theta}$ $(i=1,\cdots,n)$ 矛盾．

於是可知 C' 中除原點外無整點．由定理 2.1，有

$$\frac{2^n\{1+(1-\theta)^2\}^{n/2}}{|D|} \leqslant 2^n,$$

即

$$\left\{1+(1-\theta)^2\right\}^{n/2} \leqslant \frac{1-\theta}{m}.$$

當 $\varepsilon \to 0$ 時，$\theta \to 0$，卽得

$$m \leqslant 2^{-\frac{n}{2}}.$$

§10. 在代數數論上的應用.

命 $\omega_1,\cdots,\omega_n$ 爲 n 次代數數域 $R(\vartheta)$ 的一組整底，若於 $\vartheta^{(1)},\cdots,\vartheta^{(n)}$ 中有 r_1 個實數，r_2 對共軛複數，$r_1+2r_2=n$，則易見下面 n 個線性型

$$\alpha^{(i)} = \omega_1^{(i)} x_1 + \cdots + \omega_n^{(i)} x_n \qquad (i=1,2,\cdots,n)$$

內有 r_1 個具有實係數,有 r_2 對具有共軛複數作爲係數. 又易見此組線性方程的係數行列式的絕對值爲 $\sqrt{|\Delta|}$, Δ 爲域 $R(\vartheta)$ 的基數. 命 $\alpha=\alpha^{(1)}$, 在定理 8.1 中,取 $\sigma=1$, 可知有一組不全等於零的有理整數 $x_1,\cdots,x_n$ 使

$$|N(\alpha)|^{1/n}\leqslant\frac{1}{n}\sum_{i=1}^{n}|\alpha^{(i)}|\leqslant\left(\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|\Delta|}\right)^{1/n},$$

亦卽在 $R(\vartheta)$ 中有一不爲零的代數整數 α 適合

$$|N(\alpha)|\leqslant\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|\Delta|}. \tag{1}$$

但 $|N(\alpha)|$ 爲一自然數,又因 $2r_2\leqslant n$, 所以

$$\sqrt{|\Delta|}\geqslant\left(\frac{\pi}{4}\right)^{r_2}\frac{n^n}{n!}\geqslant\left(\frac{\pi}{4}\right)^{n/2}\frac{n^n}{n!}. \tag{2}$$

命 $v_n=\left(\frac{\pi}{4}\right)^{\frac{n}{2}}\frac{n^n}{n!}$, 則

$$\frac{v_{n+1}}{v_n}=\frac{\sqrt{\pi}}{2}\left(1+\frac{1}{n}\right)^n\geqslant\pi^{1/2}>1.$$

所以 $\{v_n\}$ 爲一遞增而趨向無窮的數列. 又當 $n=2$ 時,

$$\sqrt{|\Delta|}\geqslant v_2=\frac{\pi}{2}>1.$$

故得:

定理 1. 僅在有理數域內,基數等於 1.

及

定理 2. 若 Δ 爲一有理整數,則必有一有限數 $n(\Delta)$, 使凡基數爲 Δ 的代數數域的次數均不大於 $n(\Delta)$.

不但如此,更可進一步,證明:

定理 3. 對於固定的有理整數 Δ, 至多僅有有限個代數數域以 Δ 爲基數.

證: 由定理 2, 祇須證明,對任何自然數 n, n 次域之有基數爲 Δ 者,其個數有限.

若 $R(\vartheta)$ 爲一個基數爲 Δ 的 n 次域, $\omega_1,\cdots,\omega_n$ 爲它的一組整底. 命

$$\alpha^{(i)}=\omega_1^{(i)}x_1+\cdots+\omega_n^{(i)}x_n\qquad(i=1,\cdots,n),$$

並定義 r_1, r_2 如前. 不失普遍性地可以假定 $\alpha^{(1)}=\alpha, \alpha^{(2)}, \cdots, \alpha^{(r_1)}$ 具有實係數, $\alpha^{(r_1+1)}, \cdots, \alpha^{(n)}$ 具有複係數,且 $\overline{\alpha^{(r_1+\nu)}}=\alpha^{(r_1+r_2+\nu)}$,其中 $1\leqslant\nu\leqslant r_2$. 命

$$\alpha^{(\nu)}=\eta_\nu \qquad (1\leqslant\nu\leqslant r_1),$$

$$\alpha^{(r_1+\nu)}=\eta_{r_1+\nu}+i\,\eta_{r_1+r_2+\nu} \qquad (1\leqslant\nu\leqslant r_2),$$

則由定理 8.3, 可知有一組不全等於 0 的有理整數 $x_1^*, \cdots, x_n^*$ 使

$$|\eta_1^*|\leqslant\frac{1}{2}, \cdots, |\eta_{n-1}^*|\leqslant\frac{1}{2}, |\eta_n^*|\leqslant 2^{n-1}\sqrt{|\Delta|}. \tag{3}$$

於是有常數 c, c 僅與 n 有關,使

$$|\alpha^{*(i)}|<c\sqrt{|\Delta|} \qquad (i=1,2,\cdots,n). \tag{4}$$

若能證明

$$\alpha^{*(n)}\neq\alpha^{*(i)} \qquad (i=1,\cdots,n-1),$$

則由定理 16.3.1 可知 α^* 為一 n 次代數數,且易證 $R(\vartheta)=R(\alpha^*)$. 命 α^* 所適合的不可化方程為

$$f(x)=x^n+a_1x^{n-1}+\cdots+a_n=0, \tag{5}$$

則諸 a_k 必須適合

$$|a_k|\leqslant\binom{n}{k}(c\sqrt{|\Delta|})^k \qquad (k=1,\cdots,n). \tag{6}$$

因此任何具有基數為 Δ 的 n 次域 $R(\vartheta)$ 必與某一 $R(\alpha^*)$ 同,而 α^* 為某一適合條件 (6) 的不可化方程 (5) 的根. 因為這種不可化方程的個數有限,於是就得到定理. 因此最後祇需證明

$$\alpha^{*(n)}\neq\alpha^{*(i)} \qquad (i=1,\cdots,n-1) \tag{7}$$

的成立.

若 $r_2=0$, 則 $\alpha^{*(\nu)}=\eta_\nu^*$ $(\nu=1,\cdots,n)$. 由 (3) 式可知

$$1\leqslant|N(\alpha^*)|\leqslant\frac{1}{2^{n-1}}|\alpha^{*(n)}|.$$

但

$$|\alpha^{*(i)}|\leqslant\frac{1}{2}<2^{n-1}\leqslant|\alpha^{*(n)}| \qquad (i=1,\cdots,n-1),$$

所以 (7) 式成立.

若 $r_2>0$, 則當 $1\leqslant\nu\leqslant r_2-1$ 時,

$$|\alpha^{*(r_1+\nu)}| = |\eta^*_{r_1+\nu} + i\eta^*_{r_1+r_2+\nu}| \leqslant \frac{1}{\sqrt{2}},$$

$$|\alpha^{*(r_1+r_2+\nu)}| = |\eta^*_{r_1+\nu} - i\eta^*_{r_1+r_2+\nu}| \leqslant \frac{1}{\sqrt{2}}.$$

於是

$$1 \leqslant |N(\alpha^*)| \leqslant \frac{1}{(\sqrt{2})^{n-2}} |\alpha^{*(n)}|^2.$$

但

$$|\alpha^{*(i)}| \leqslant \frac{1}{\sqrt{2}} < 2^{\frac{1}{4}(n-2)} \leqslant |\alpha^{*(n)}|, \qquad i \neq n,\ i \neq r_1 + r_2,$$

而 $\alpha^{*(r_1+r_2)} \neq \alpha^{*(n)}$，蓋否則將有 $\eta^*_n = 0$，於是 $|\alpha^{*(n)}| \leqslant \frac{1}{2}$，而得

$$1 \leqslant |N(\alpha^*)| \leqslant \frac{1}{(\sqrt{2})^{n+2}}.$$

但此爲不可能之事. 故當 $r_2 > 0$ 時，(7) 式也成立. 定理得證.

習題 1. 證明在一理想數 $\mathfrak{A}$ 中可以選得一整數 α，使

$$|N(\alpha)| \leqslant \sqrt{|\Delta|}\, N(\mathfrak{A}).$$

習題 2. 證明任一理想數類中有一理想數 $\mathfrak{A}$ 適合於

$$N(\mathfrak{A}) \leqslant \sqrt{|\Delta|}.$$

§11. $|\Delta|$ 的極小值.

在上一節內我們看到 n 次代數數域的基數 Δ，適合

$$|\Delta| \geqslant \left(\frac{\pi}{4}\right)^{2r_2} \left(\frac{n^n}{n!}\right)^2.$$

再由 $\Delta \equiv 0$ 或 $1 \pmod 4$，及 $(-1)^{r_2}\Delta > 0$ 的性質，可以作出下表：

	$r_2 = 0$	$r_2 = 1$	$r_2 = 2$
$n = 2$	$\Delta \geqslant 4$	$\Delta \leqslant -3$	—
$n = 3$	$\Delta \geqslant 21$	$\Delta \leqslant -15$	—
$n = 4$	$\Delta \geqslant 116$	$\Delta \leqslant -71$	$\Delta \geqslant 44$
$n = 5$	$\Delta \geqslant 680$	$\Delta \leqslant -419$	$\Delta \geqslant 260$

(I)

但經實際計算得出 $|\Delta|$ 之極小值爲

	$r_2=0$	$r_2=1$	$r_2=2$
$n=2$	$\Delta=5$	$\Delta=-3$	——
$n=3$	$\Delta=49$	$\Delta=-23$	——
$n=4$	$\Delta=725$	$\Delta=-275$	$\Delta=117$

(II)

由二次域 $R(\sqrt{5})$, $R(\sqrt{-3})$ 即得表 (II) 中 $n=2$ 的情形.

對於 $n=3$ 的情形,若 ϑ 適合 $x^3+x^2-2x-1=0$, 則 $R(\vartheta)$ 的基數卽爲 49, 而若 ϑ 適合 $x^3-x-1=0$, 則 $R(\vartheta)$ 的基數爲 -23.

至於 $n=4$ 的情形,命 ϑ 爲 $x^4-2ax^2+(-1)^{\frac{1}{2}(p-1)}p=0$ 的根. 可以證明:

1) 當 $a=7$, $p=29$ 時, 可得 $r_2=0$, $\Delta=725$;

2) 當 $a=3$, $p=11$ 時, 可得 $r_2=1$, $\Delta=-275$;

3) 當 $a=-1$, $p=13$ 時, 可得 $r_2=2$, $\Delta=117$.

如何作出表 (II) 是一個問題. 表中 $n=2$ 的情形可以很容易地得到. 但當 $n\geqslant 3$ 時,雖然定理 10.3 的證明供給了一個方法,可以經過"有限次"的計算,求出表 (II) 中所列的結果,但在實際計算時,用此方法必須求出數以千計的多項式之根, 以及由它們所決定的代數數域的基數. 因此可見在解決具體問題時,尙須有賴於具體的方法. 今舉 $n=3$ 的情形而考察之.

假定我們所討論之三次域 $R(\vartheta)$ 的基數 Δ 適合於 $0<\Delta\leqslant 49$ $(r_2=0)$, 或 $-23\leqslant\Delta<0$ $(r_2=1)$. 由 §10 可知在此域中有一非 0 的整數 α 使

$$|\alpha^{(1)}|+|\alpha^{(2)}|+|\alpha^{(3)}|\leqslant\tau, \tag{1}$$

而

$$3<\tau=\begin{cases}42^{1/3}, \\ 2\left(\dfrac{3}{\pi}\right)^{1/3}23^{1/6}.\end{cases}$$

α 的次數爲 3 或 1. 假如能够確定 α 的次數爲 3, 亦卽 α 決不爲有理整數, 那末 $R(\vartheta)=R(\alpha)$, 而由不等式 (1) 可以確定 α 所適合的方程式係數的範圍, 從而經過有限次的計算或能得到結果. 但很不幸的是我們沒有辦法確定 α 不可能是有理整數. 相反的,由於 $\tau>3$, 所以 $\alpha=\pm 1$ 適合 (1) 式,而 ± 1 在 $R(\vartheta)$ 中;所以此法不能適用.

令 ρ 爲一大於 3 的正數，而考慮凸體 B:

$$\begin{cases} |\xi_1| + |\xi_2| + |\xi_3| \leqslant \rho, \\ |\xi_1 + \xi_2 + \xi_3| < 3(<\rho), \end{cases}$$

其中

$$\xi_i = \omega_1^{(i)} x_1 + \omega_2^{(i)} x_2 + \omega_3^{(i)} x_3,$$

而 $\omega_1, \omega_2, \omega_3$ 爲 $R(\vartheta)$ 的一組整底．易見 B 爲一個以原點爲對稱中心的凸體．

命凸體 A:

$$|\xi_1| + |\xi_2| + |\xi_3| \leqslant \rho$$

被平面 $\xi_1 + \xi_2 + \xi_3 = t$ 截後所得截面的面積爲 $F(t)$．則 $F(t) = F(-t)$，且當 $t \geqslant 0$ 時，$F(t)$ 爲遞減的．於是

$$B \text{ 的體積} = 2\int_0^3 F(t)\, dt = 2\frac{3}{\rho}\int_0^\rho F\left(\frac{3}{\rho}u\right) du \geqslant$$

$$\geqslant 2\frac{3}{\rho}\int_0^\rho F(u)\, du = \frac{3}{\rho} \times A \text{ 的體積}.$$

但

$$A \text{ 的體積} = \begin{cases} 2^3 \dfrac{\rho^3}{3!\sqrt{49}}, & \text{當 } r_2 = 0; \\ 2^3 \left(\dfrac{\pi}{4}\right) \dfrac{\rho^3}{3!} \dfrac{1}{\sqrt{23}}, & \text{當 } r_2 = 1. \end{cases}$$

故由 Minkowski 定理，在 $R(\vartheta)$ 內有一不等於 0 的整數 α 適合

$$|\alpha^{(1)}| + |\alpha^{(2)}| + |\alpha^{(3)}| \leqslant \tau' = \begin{cases} \sqrt{14}, & \text{當 } r_2 = 0; \\ \sqrt{\dfrac{8}{\pi}\sqrt{23}}, & \text{當 } r_2 = 1 \end{cases} \tag{2}$$

及

$$|\alpha^{(1)} + \alpha^{(2)} + \alpha^{(3)}| < 3. \tag{3}$$

並由 (3) 式可知 α 決不是有理整數．所以 α 的次數爲 3，於是 $R(\vartheta) = R(\alpha)$．命 α 所適合的不可化方程爲

$$f(x) = x^3 - g_1 x^2 + g_2 x - g_3 = 0. \tag{4}$$

則 $g_3 \neq 0$，且可假定 $g_3 > 0$．蓋若不然，則因 $-\alpha$ 適合

$$g(x)=x^3-(-g_1)x^2+g_2x-(-g_3)=0,$$

而 $R(\vartheta)=R(\alpha)=R(-\alpha)$，且 $-\alpha$ 適合 (2) 式及 (3) 式，所以不妨假定 $g_3>0$。

由根與係數的關係

$$|g_1|=|\alpha^{(1)}+\alpha^{(2)}+\alpha^{(3)}|<3,$$

$$g_3=\alpha^{(1)}\alpha^{(2)}\alpha^{(3)}\leqslant\left(\frac{|\alpha^{(1)}|+|\alpha^{(2)}|+|\alpha^{(3)}|}{3}\right)^3<2,$$

所以 $|g_1|\leqslant 2$，$g_3=1$。最後祇須求出 g_2 所在之範圍，

$$\begin{aligned}|g_2|&=|\alpha^{(1)}\alpha^{(2)}+\alpha^{(1)}\alpha^{(3)}+\alpha^{(2)}\alpha^{(3)}|\leqslant\\&\leqslant|\alpha^{(1)}\alpha^{(2)}|+|\alpha^{(1)}\alpha^{(3)}|+|\alpha^{(2)}\alpha^{(3)}|\leqslant\\&\leqslant\frac{(|\alpha^{(1)}|+|\alpha^{(2)}|+|\alpha^{(3)}|)^2}{3}\leqslant\frac{\tau'^2}{3}<5,\end{aligned}$$

所以 $|g_2|\leqslant 4$。但當 $r_2=0$ 時，我們可以計算得 $|g_2|\leqslant 3$。蓋因此時 $\alpha^{(i)}$ $(i=1,2,3)$ 全為實數，故或則三者同號，或則其中有二者同號，而與另一異號。對於第一種情形，

$$\begin{aligned}|g_2|&\leqslant|\alpha^{(1)}\alpha^{(2)}|+|\alpha^{(1)}\alpha^{(3)}|+|\alpha^{(2)}\alpha^{(3)}|\leqslant\\&\leqslant\frac{(|\alpha^{(1)}|+|\alpha^{(2)}|+|\alpha^{(3)}|)^2}{3}=\frac{(\alpha^{(1)}+\alpha^{(2)}+\alpha^{(3)})^2}{3}<3,\end{aligned}$$

而對第二種情形，不妨假定 $\alpha^{(1)}\alpha^{(2)}>0$，$\alpha^{(1)}\alpha^{(3)}<0$，於是

$$\begin{aligned}|g_2|&\leqslant|\alpha^{(1)}\alpha^{(2)}+\alpha^{(1)}\alpha^{(3)}+\alpha^{(2)}\alpha^{(3)}|\leqslant\\&\leqslant\max(\alpha^{(1)}\alpha^{(2)},-\alpha^{(3)}(\alpha^{(1)}+\alpha^{(2)}))\leqslant\\&\leqslant\left(\frac{\alpha^{(1)}+\alpha^{(2)}-\alpha^{(3)}}{2}\right)^2\leqslant\frac{14}{4}<4,\end{aligned}$$

亦即 $|g_2|\leqslant 3$。

總結以上所述，可知，在任一基數 Δ 適合 $0<\Delta\leqslant 49$ $(r_2=0)$ 或 $-23\leqslant\Delta<0$ $(r_2=1)$ 的三次域 $R(\vartheta)$ 中可找到一整數 α，使 $R(\vartheta)=R(\alpha)$，而 α 滿足形如

$$x^3-g_1x^2+g_2x-1=0$$

的不可化方程，其中 $|g_1|\leqslant 2$，$|g_2|\leqslant 4$（當 $r_2=0$ 時，$|g_2|\leqslant 3$）。所以若

要求出所有基數 Δ 適合 $0 < \Delta \leqslant 49 (r_2 = 0)$ 或 $-23 \leqslant \Delta < 0$ 的三次域 $R(\vartheta)$，衹須考慮所有這種方程即可．但這種方程的個數至多不超過 45 個 ($r_2 = 0$ 時,不超過 35 個),並且當 $g_1 = g_2$ 時,方程有根 1，當 $g_1 + g_2 + 2 = 0$ 時,方程有根 -1．對於這種情形,方程爲可化,故不必考慮．又因 $x^3 - g_2 x^2 + g_1 x - 1 = 0$ 的根爲 $x^3 - g_1 x^2 + g_2 x - 1 = 0$ 的根的倒數，而 $R(\vartheta) = R\left(\frac{1}{\vartheta}\right)$，所以 (4) 的倒數方程也就不必考慮．因此最後衹須考慮 27 個 ($r_2 = 0$ 時爲 18 個)方程．求出此 27 個(或 18 個)方程的根 ϑ，再定出 $R(\vartheta)$ 的基數,即得表 (II) 上 $n = 3$ 的結果．

參考書目

[1] 李儼,中算史論叢(五卷,科學出版社, 1954—1955).

[2] 吳在淵,數論初步(商務印書館, 1931).

[3] 胡濬濟,數論(商務印書館, 1928).

[4] 華羅庚,堆壘素數論(中國科學院, 1953).

[5] 高木貞治,初等整數論講義(東京, 1931).

[6] 高木貞治,代數的整數論(東京, 1948).

[7] Виноградов, И. М., Основы теории чисел (Гостехиздат, 1949) (有中譯本"數論基礎", 裘光明譯,高等教育出版社).

[8] Виноградов, И. М., Метод тригонометрических сумм в теории чисел (Труды Матем. института им. В. А. Стеклова, т. 23, стр. 1-109, 重印入 И. М. Виноградов 的 Избранные труды 中) (有中譯本"數論中的三角和法", 越民義譯,見數學進展第 1 卷 (1955) 3—106 頁).

[9] Гельфонд, А. О., Трансцендентные и алгебраические числа (Гостехиздат, Москва, 1952).

[10] Чудаков, Н. Г., Введение в теорию L-функций Дирихле (Гостехиздат, 1947, Москва-Ленинград).

[11] Хинчин, А. Я., Три жемчужины теории чисел (Гостехиздат, Москва).

[12] Bachmann, P., Niedere Zahlentheorie (Leipzig, Teubner, Teil 1, 1902; Teil 2, 1910).

[13] Chamichael, R. D., Theory of numbers (Mathematical Monographs, no. 13, New York, Wiley, 1914).

[14] Chamichael, R. D., Diophantine analysis (Mathematical Monographs, no. 16, New York, Wiley, 1915).

[15] Dickson, L. E., Introduction to the theory of numbers (Chicago Univ. Press, 1929; Introduction).

[16] Dickson, L. E., History of the theory of numbers (Carnegie Institution, vol. i, 1919; vol. ii, 1920; vol. iii, 1923; History).

[17] Lejeune Dirichlet, P. G., Vorlesungen über Zahlentheorie, herausgeben von R. Dedekind (4. Auflage, Braunschweig, Vieweg, 1894).

[18] Estermann, T., Introduction to modern prime number theory (Cambridge Tracts in Mathematics, no. 41, 1952).

[19] Gauss, C. F., Disquisitiones arithmeticae (Leipzig, Fleishcer, 1801,重印入 Gauss 的 Werke 的卷 1 中).

[20] Hardy, G. H. and Wright, E. M., An introduction to the theory of numbers (3rd edition, Oxford, 1954).

[21] Hasse, H., Zahlentheorie (Berlin Akademie-Verlag, 1949).

[22] Hasse, H., Vorlesungen über Zahlentheorie (Berlin, Springer, 1950).

[23] Hecke, H., Vorlesungen über die Theorie der algebraischen Zahlen (Leipzig, Akademische Verlagsgesellschaft, 1923).

[24] Hilbert, D., Bericht über die Theorie der algebraischen Zahlkörper (Jahresbericht der Deutschen Mathematiker-Vereinigung, iv, 1897, 重印入 Hilbert 的 Gesammelte Abhandlungen 的卷 1 中)

[25] Ingham, A. E., The distribution of prime numbers (Cambridge Tracts in Mathematics, no. 30, Cambridge Univ. Press, 1932).

[26] Koksma, J. F., Diophantische Approximationen (Ergebnisse der Mathematik, Band iv, Heft 4, Berlin, Springer, 1937).

[27] Kraitchik, M., Introduction à la théorie des nombres (Paris, 1952).

[28] Landau, E., Handbuch der Lehre von der Verteilung der Primzahlen (2 Bände, Leipzig, Teubner, 1909; Handbuch).

[29] Landau, E., Vorlesungen über Zahlentheorie (3 Bände, Leipzig, Hirzel, 1927; Vorlesungen).

[30] Landau, E., Über einige neuere Fortschritte der additiven Zahlentheorie (Cambridge Tracts in Mathematics, no. 35, Combridge Univ. Press, 1937).

[31] Landau, E., Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale (2. Auflage, Leipzig, Teubner, 1927; Algebraische Zahlen).

[32] Mathews, G. B., Theory of numbers (Cambridge, Deighton Bell, 1892).

[33] Minkowski, H., Geometrie der Zahlen (Leipzig, Teubner, 1910).

[34] Minkowski, H., Diophantische Approximationen (Leipzig, Teubner, 1927).

[35] Nagell, T., Introduction to number theory (New York, 1951).

[36] Ostmann, H. H., Additive Zahlentheorie (2 Bände, Springer-Verlag, Berlin, 1956).

[37] Perron, O., Irrationalzahlen (Berlin, de Gruyter, 1910).

[38] Perron, O., Die Lehre von den Kettenbrüchen (Leipzig, Teubner, 1929).

[39] Polya, G. und Szego, G., Aufgaben und Lehrsätze aus der Analysis (2 Bände, Berlin, Springer, 1925).

[40] Rademacher, H. und Toeplitz, O., Von Zahlen und Figuren (2. Auflage, Berlin, Springer, 1933).

[41] Siegel, C. L., Transcendental numbers (Princeton Univ. Press, 1949).

[42] Sierpinski, W., Teoria Liezb (Warszawa-Wroclaw, 1950).

[43] Skolem, T., Diophantische Gleichungen (Ergebnisse, Springer, 1937).

[44] Sommer, J., Vorlesungen über Zahlentheorie (Leipzig, Teubner, 1907).

[45] Titchmarsh, E. C., The theory of the Riemann zeta-function (Oxford, 1951).

[46] Turan, P., Eine neue Methode in der Analysis und deren Anwendungen (Akademiai Kiado, Budabest, 1953),(有中譯本,"數學分析中的一個新方法及其應用", 郭煥庭譯,見數學進展第2卷 (1956) 312—365 頁).

名詞索引

一 畫

一致分佈	uniform distribution	однообразный распределение	§10.12

四 畫

公式	formula	формула	§6.3
Möbius 反轉 ~	Möbius inversion ~		
Euler ~			§8.3
Selberg ~			§9.6
分拆	partition	разделение	§8.1
共軛 ~	conjugate ~	сопряженное ~	§8.5
自共軛 ~	self-conjugate ~	самосопряженное ~	§8.5
奇 ~	odd ~	нечётное ~	§8.5
偶 ~	even ~	чётное ~	§8.5
~ 之圖解	graph of ~	чертёж ~	§8.5
分解式	factorization, decomposition	представление	
自然數之標準~	standard ~ of a natural number	каноническое~целых	§1.2
特徵的標準 ~	standard ~ of a character	каноническое ~ характера	§7.2
方法	method	метод	
Euler-Binet ~			§11.9
Selberg ~			§19.1
方陣	square matrix	квадратная матрица	§14.1
對角線 ~	diagonal matrix	диагональная матрица	§14.2
伴隨 ~	adjoint ~	присоединенная ~	§14.2
伴隨模 ~	adjoint unimodular ~	присоединенная модулярная ~	§14.7
初等變換 ~	elementary ~	элементарная ~	§14.2
(非)奇異 ~	(non) singular ~	(не) особенная ~	§14.1
逆 ~	inverse ~	обратная ~	§14.1
素~，不可分解~	prime ~	простая ~	§14.7

標準素 ~	standard prime ~	нормальная простая ~	§14.7
單位 ~	unit ~	единичная ~	§14.1
零 ~	null ~	нулевая ~	§14.1
複合 ~	composite ~	составная ~	§14.7
模 ~	modular ~	модулярная ~	§14.1
~ 的左結合標準形式	normal form(of Hermite)	нормальная форма	§14.1
~ 的相似標準形式	normal form (of Smith)	нормальная форма	§14.1
方程	equation	уравнение	
一次不定 ~	linear diophantine ~	линейное неопределенное ~	§1.8
二次不定 ~	quadratic diophantine ~	~второй степени с двумя неизвестными	§11.3
Diophantus ~			§11.1
Марков ~			§11.8
Pell ~			§10.9
不等式	inequality	неравенство	
Буняковский-Schwarz ~			§18.7
Hölder ~			§20.7
Minkowski ~			§20.7
Selberg ~			§19.4
引	lemma	лемма	
Gauss ~			§3.2
比	ratio	отношение	
交 ~	cross ~	сложное ~	§13.3

五 畫

對合	involution	инволуция	§13.2
未定量	indeterminante	неопределённый	§14.9
矢量	vector	вестор	§13.1
平面	plane	плоскость	
複虛數 ~	complex ~	комплексная ~	§13.1

六 畫

交	intersection	пересечение	§14.9
因子	factor, divisor	множитель, делитель	
不變 ~	invariant factor	инвариантный множитель	§14.5

初等 ~	elementary divisor	элементарный делитель	§14.5
重 ~	multiple factor	многократный множитель	§4.6
多項式	polynomial	многочлен	
(不)可化 ~	(ir) reducible ~	(не) приводимый ~	§1.13
對模 p 不可化 ~ (對模 p 素 ~)	irreducible ~ respect to modulus p	неприводимый ~ по модулем p	§4.5
整值 ~	integral valued ~	целочисленный ~	§1.12
次數	degree	степень	
代數數的 ~	~ of an algebraic number	~ алгебраического числа	§16.1
曲面	surface	поверхность	
三次 ~	cubic ~	кубическая ~	§11.10
φ-收斂	φ-convergence	φ-сходимость	§15.6
同餘式	congruence	сравнение	
一次 ~	linear ~	~ первой степени	§2.6
高次 ~	~ of higher degree	~ высшей степени	§2.8
多項式的 ~	~ of polynomials		§4.3
重模 ~	~ respect to double modulus	~ по двоиным модулям	§4.7
理想數的 ~	~ with respect to modulus ideal	~ по модулям идеала	§16.9
同餘類	residue class	класс вычета	§2.2
同冪	equivalent	эквивалент	§17.1

七 畫

判別式	discriminant	дискриминант	§12.1
基本 ~	fundamental ~	фундментальный ~	§12.11
判別條件	criterion	критерий	
一致分佈之 ~	~ for uniform distribution	~ для однообразное распределение	§10.12
Euler ~			§3.1
Legendre ~			§10.7
Lucas' ~, Lucas' test			§16.15
餘子式	cofactor	дополнение	§14.2
代數 ~	algebraic ~	алгебраическое ~	§14.2

系(系統)	system	система	
完全剩餘 ~	complete residue ~	~ полных вычетов	§2.2
特徵 ~	~ of characters	~ характеров	§12.6
縮(剩餘) ~	reduced residue ~	~ приведённых вычетов	§2.3
p-adic 數 ~	p-adic number ~	~ p-адических чисел	§15.6

八畫

長度	length	длина	
非歐 ~	non-euclidean ~	Неевклидовая ~	§13.4
表示論	theory of representation	теория представления	§7.1
函數	function	функция	
對數 ~	logarithmic ~	логарифмическая ~	§5.2
遞減 ~	decreasing ~	убывающая ~	§5.8
遞增 ~	increasing ~	возрастающая ~	§5.8
Euler ~			§2.3
特徵 ~	characteristic ~	характерная ~	§7.2
對稱 ~	symmetric ~	симметрическая ~	§7.10
數論 ~	arithmetical ~	арифметическая ~	§6.1
積性 ~	multiplicative ~	мультипликативная ~	§6.1
完全積性 ~	complete multiplicative ~	полная мультипликативная ~	§6.1
Möbius ~			§6.1
Von Mangoldt ~			§6.1
除數 ~	divisor ~	~ делителей	§6.1
演成 ~	generating ~	полождающая ~	§6.14
Riemann Zeta ~			§6.14
Чебышев ~			§9.1
慢遞減 ~	slowly decreasing ~	медленно убывающая ~	§9.4
橢圓模 ~	elliptic modular ~	эллиптическая модулярная ~	§8.1
表示法	representation	представление	
分式 ~	decomposition into partial fractions	разложение в частных дроби	§8.4
p-adic ~	p-adic representation	p-адическое представление	§15.1

和	sum	сумма	
三角 ~	trigonometric ~	тригонометрическая ~	§7.5
(不)完整 ~	(in) complete ~	(не) полная ~	§7.7
等冪 ~	~ of equal powers		§18.6
Gauss ~			§7.5
和(集的 ~)	union	единение	§14.9
底(基底)	base	базис	
標準 ~	canonical ~	~ в каноническом форме	§14.9; §16.8
域的 ~	~ of field	~ поля	§16.3
整 ~	integral ~	целочисленный ~	§16.4
定理	theorem,	теорема	
唯一分解 ~	unique factorization ~	~ единственности разложения	§1.5
素數 ~	prime number ~	асимптотический закон распределения простых чисел	§9.1
商高 ~			§11.1
孫子 ~	Chinese remainder ~		§2.7
Cauchy ~			§18.3
Dirichlet ~			§5.12; §9.8
Eisenstein ~			§1.13
Euler ~			§2.3
Fermat ~			§1.12
Gauss ~			§1.13
Gauss 互逆 ~	~ law of reciprocity	закон взаимности	§3.3
Hensel ~			§15.9
Hermite ~			§17.6
Hurwitz ~			§10.4
Hilbert ~			§4.4
Ikehara ~			§9.4
Lagrange ~			§8.7
Landau-Ostrowski-Thue ~			§17.5
Lindemann ~			§17.7
Liouville ~			§17.2
Littlewood ~			§5.3
Mann ~			§19.2

Mayer ~			§11.6
Pólya ~			§7.7
Roth ~			§17.4
Siegel ~			§17.3
Sierpinski ~			§6.12
Tauber 型 ~	Tauberian ~		§9.4
Thue ~			§17.4
Waring-Hilbert ~			§19.1; §19.6
Wilson ~			§2.9
Wolstenholme ~			§2.10
Виноградов ~			§6.11; §7.7
Вороной ~			§6.12
Гельфонд ~			§17.8
Гольдбах-Шнирельман ~			§19.1; §19.3
Горшков ~			§7.8
Чебышев ~			§5.3; §5.6; §5.9; §10.10
Хинчин ~			§10.10

九 畫

恆等式	identity	тождество	
Euler ~			§5.4
Jacobi ~			§8.7
指數	index	индекс	§3.8
點	point	точка	
定 ~	fixed ~	неподвижная ~	§13.2
既約 ~	reduced ~	приведённая ~	§13.6
無窮遠 ~	~ at infinity	бесконечно удалённая ~	§13.1
整 ~	lattice ~	целая ~	§3.3
型	form	форма	
二元二次 ~	binary quadratic ~	бинарная квадратичная ~	§12.1
已化 ~	reduced ~	приведённая ~	§12.2
不定 ~	indefinite ~	неопределённые ~	§12.1
定正 ~	positive (definite) ~	положительные (определённые) ~	§12.1
定負 ~	negative (definite) ~	отрицательные (определённые) ~	§12.1
非原 ~	imprimitive ~	непервообразная ~	§12.4

原 ~	primitive ~	первообразное ~	§12.4
相似二次 ~	equivalent ~	эквивалентное ~	§12.1

十 畫

除盡	divisibility	делимость	
左(右) ~	left (right) ~	левая (правая) ~	§14.7
逐步淘汰原則	Eratosthenes' sieve method		§1.7
原根	primitive root	первообразный корень	§3.8; §4.10
~ 之分佈問題	distribution of ~	распределение ~	§7.9
矩	norm	норма	§14.9
矩陣	matrix	матрица	§14.2
特徵	character	характер	§7.2
主 ~	principal ~	главный ~	§7.2
原 ~	primitive ~	первообразный ~	§7.3
非原 ~	improper ~	производный ~	§7.3
實 ~	real ~	действительный ~	§7.3
~ 和	~ sum	сумма ~	§7.4
問題	problem,	проблем	
平方和 ~	~ on sum of squares	~от суммы квадратов	§8.7
Гольдбах ~			§5.3
Hilbert 第七 ~	the seventh ~ of Hilbert		§17.6
Prouhet ~			§18.1
Waring ~			§18.1
圓內整點 ~	circle ~		§6.9
Dirichlet 除數 ~	Dirichlet divisor ~		§6.12
級數	series; progression	ряд, прогрессия	
等差 ~	arithmetic ~	арифметическая ~	§5.12
循環冪 ~	recurring power ~	периодический степенный ~	§15.8
Dirichlet ~			§6.14
Lambert ~			§6.15
Farey 貫	Farey ~		§6.10

十 一 畫

族	genus	род	§12.6
球	sphere	шар	
Neumann ~			
商	quotient	частное	§13.1

完全 ~	complete ~	полное ~	§10.2
域	field	поле	§4.11
二次 ~	quadratic ~	квадратичное ~	§16.2
n 次代表數 ~	algebraic ~ of degree n	алгебраическое ~ порядка n	§16.2
單 ~	simple ~	простое ~	§16.14
歐基里得 ~	euclidean ~		§16.14
基 ~	fundamental region	фундаментальная область	§13.6
連分數	continued fraction	цепная дробь	§10.1
循環 ~	periodic ~	периодический ~	§10.6
密率	density	плотность	
p ~			§8.8
正 ~	positive ~	положительная ~	§19.1
實 ~	real ~	действительная ~	§8.8
理想集合	ideal	идеал	§4.1
假設,猜測	postulate, conjecture	постулат	
Bertrand ~			§5.3; §5.7
Fermat ~			§11.7
常數	constant	постоянное	
Euler's ~			§5.8; §17.6
理想數	ideal	идеал	
主 ~	principal ~	главный ~	§16.6
素 ~	prime ~	простой ~	§16.7
符號	symbol	символ	
Jacobi ~			§3.6
Kronecker ~			§12.3
Legendre ~			§3.1

十 二 畫

週期	period	период	§7.7
變換之 ~	~ of transformation	~ преобразования	§13.2
集	set	множенство	
和 ~	Union of ~	сумма ~	§19.2
距	norm	норм	§16.3
理想數的 ~	~ of ideals	~ идеала	§16.9
插入公式	interpolation formula	интерполяционная формула	§4.3

最大公因數	greatest common divisor	общий наибольший делитель	§1.4
最小公倍數	least common multiple	общее наименьшее кратное	§1.6
測地線	geodesic	геодезическая линия	§13.4
結合	association	ассоциация	§4.1
左 ~	left ~	левая ~	§14.1
右 ~	right ~	правая ~	§14.1
貫	series, sequence	последовательность	
Fibonacci ~			§10.1
基 ~	fundamental ~	фундаментальная ~	§15.6
φ-收斂 ~	φ-convergent ~	φ-сходящаяся ~	§15.6
零 ~	null ~	нулевая ~	§15.6
最大公約式(多項式之 ~)	greatest common factor (of polynomials)	общий наибольший делитель (полиномов)	§4.1
最小公倍式(多項式之 ~)	least common multiple (of polynomials)	общее наименьшее делитель (полиномов)	§4.2
階	order	порядок	
無窮大之 ~	order of infinity	~ бесконечности	§5.1
剩餘	residue	вычет	
二次(非) ~	quadratic (non-) ~	квадратичный (не-) ~	§3.1
k 次(非) ~	(non-)~ of k-th degree	(не-) ~ степени k	§3.8
項	term	член	
鄰 ~	successive ~		§6.10
中 ~	mediant		§6.10

十 三 畫

跡	trace	след	§16.3
解	solution	решение	
Fermat ~			§2.4
p-adic ~,		p-адическое ~.	§15.1
既約 ~	proper ~	приведённое ~	§11.4
原 ~	primary ~	первоначальное ~	§11.4
羣	group	группа	§13.2
Abelian ~			§4.11
伴隨 ~	adjoint ~	присоединенная ~	§14.7
φ-極限	φ-limit	φ-предел	§15.6

十 四 畫

圖解法	graphical method	графический метод	§8.5
圖形	graph	чертёж	
自共軛 ~	self-conjugate ~	самосопряженый ~	§8.5
漸近分數	convergent	подходящая дробь	§10.1
相似	equivalence	эквивалентность	
實數之 ~	~ of real numbers	~ действительной чисел	§10.5
點之 ~	~ of points	~ точек	§13.6
理想數之狹義~	~ of ideals in narrower sense	~ идеала в узном смысле	§16.13
模 q ~	~ with respect to modulus q	~ по модулем q	§12.5
遞降法	method of descent	метод понижения	§11.7

十 五 畫

模	modul	модуль	§1.4
線性 ~	linear form ~	~ линейных форм	§14.9
模方陣之演出元素	generator of modula matrices	производитель модулярных матриц	§14.3
數	number	число	
Fermat ~			§1.10
Марков ~			§10.5
Mersenne ~			§1.10
	p-adic ~	p-адическое ~	15.1
分 ~	fraction	дробь	§6.10
既約分 ~	irreducible fraction	неприводимая дробь	§6.10
無理 ~	irrational ~	иррациональное ~	§6.10
三角 ~	triangular ~	триугольное ~	§8.3
代數 ~	algebraic ~	алгебраическое ~	§16.1
代數整 ~	algebraic integer	целое алгебраическое~	§16.1
自然 ~	natural ~	натуральное ~	§1.1
共軛 ~	congugate ~	сопряженное ~	§16.3
完全 ~	perfect ~	совершенное ~	§1.9
因 ~	divisor	делитель	§1.1
奇 ~	odd	нечётное ~	§1.2
實 ~	real ~	вещественное ~	§5.11

素 ~	prime ~	простое ~	§1.2
倍 ~	multiple	кратное	§1.1
基本單位 ~	fundamental unit	фундаментальная единица	§16.11
域的基 ~	discriminant of a field	дискриминант поля	§16.4
無平方因子~	square free ~	~ не делящееся на квадрады	§6.6
偶 ~	even ~	чётное ~	§1.2
單位 ~	unit,	единица	§16.1
超越 ~	transcendental ~	трансцендентное ~	§17.1
複 ~	complex ~	комплексное ~	§7.1
複合 ~	composite ~	составное ~	§1.2
整 ~	integer ~	целое ~	§1.1
數學歸納法	mathematical induction	математическая индукция	§5.7
數論三珠	three pearls in the theory of numbers	три жемчужины теории чесел	§18.1
賦值	valuation	оценка	§15.2
恆等 ~	identical ~	одинаковая ~	§15.2
	p-idic ~	p-адическое ~	§15.2
亞基米得 ~	Archimede's ~		§15.3
非亞基米得 ~	non-Archimede's ~		§15.3
~ 的等價	equivalence of ~	эквивалентность ~	§15.3

十 六 畫

幅角	argument	аргумент	§13.1
導數	derivative	производная	§4.6
積	product	произведение	
方陣之 ~	~ of matrices	~ матриц	§13.2
變換之 ~	~ of transformations	~ преобразований	§13.2
篩法	sieve method		
Brun's ~			§19.1
Eratosthenes ~			§1.3

十 七 畫

輾轉相除法	euclidean algorithm	алгоритм эвклида	§1.4
擴張	extention	расширение	
代數 ~	algebraic ~	алгебраическое ~	§4.11
有理數之 ϕ~	ϕ~ of rational number	ϕ~ системы рацио-	

	system	нального числа	§15.6
單 ~	simple ~	простое ~	§16.2
環	ring	кольцо	§4.11

十八畫

類	class	класс	
理想數 ~	ideal ~	~ идеала	§16.12

二十二畫

孿生素數	twin primes	пара близнецов	§19.5
變換	transformation	преобразование	
有限次 ~	~ of finite order	~ конечного порядка	§13.2
單位 ~	identical ~	тождественное ~	§13.2
初等 ~	elementary ~	элементатное ~	§14.1
逆 ~	inverse ~	обратное ~	§13.1
雙曲 ~	hyperbolic ~	гиперболическое ~	§13.2
橢圓 ~	elliptic ~	эллиптическое ~	§13.2
拋物 ~	parabolic ~	параболическое ~	§13.2
等緯角 ~	loxodromic ~	локсодромические ~	§13.2
~ 之行列式	determinant of ~	определитель ~	§13.2
Möbius ~	Möbius' transform		§6.4
Möbius 逆~	Möbius' inverse transform		§6.4